

可靠性技术丛书编委会

主 任 谢少锋

副主任 王 勇 陈立辉

委 员（按姓氏笔画排序）

王晓晗 王蕴辉 刘尚文 纪春阳

张 铮 张增照 张德平 罗道军

赵国祥 胡湘洪 莫郁薇 恩云飞

潘 勇

可靠性技术丛书

可靠性概论

工业和信息化部电子第五研究所 组编

潘 勇 黄进永 胡 宁 编著

编写组成员：杨洪旗 冯燕宽 葛智君

黄智伟 张增照 周军连

陈冰泉 任 艳 张三娣

方子豪

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书紧扣可靠性工程发展脉络,深入浅出地阐述了可靠性的基础理论、常用工程技术方法和主要标准规范,探讨了可靠性工程的若干发展趋势和面临的挑战,并给出了大量的案例。全书共 11 章,内容覆盖可靠性相关概念、发展历程与趋势、产品的寿命分布、可靠性管理、要求论证、设计分析、试验评价、数据收集及分析评估等技术方法,并讨论了软件和网络可靠性问题,给出了国内/国际常用的可靠性技术标准规范。

本书适用于产品设计师、质量与可靠性管理和技术人员、从事可靠性领域的理论研究和工程服务人员参考,也可作为高等院校相关专业的教材和参考资料,以及可靠性领域的培训资料使用。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究。

图书在版编目(CIP)数据

可靠性概论/潘勇,黄进永,胡宁编著;工业和信息化部电子第五研究所组编. —北京:电子工业出版社,2015.11

(可靠性技术丛书)

ISBN 978-7-121-27240-0

I. ①可… II. ①潘… ②黄… ③胡… ④工… III. ①可靠性理论 IV. ①O213.2

中国版本图书馆 CIP 数据核字(2015)第 226086 号

策划编辑:张 榕

责任编辑:张 榕 文字编辑:张 楠

印 刷:

装 订:

出版发行:电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本:720×1 000 1/16 印张:38.75 字数:778.7 千字

版 次:2015 年 11 月第 1 版

印 次:2015 年 11 月第 1 次印刷

印 数:3 500 册 定价:118.00 元

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010) 88254888。

质量投诉请发邮件至 zltts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线:(010) 88258888。

丛 书 序

以可靠性为中心的质量是推动经济社会发展永恒的主题，关系国计民生，关乎发展大局。把质量发展放在国家和经济发展的战略位置全面推进，是国际社会普遍认同的发展规律。加快实施制造强国建设，必须牢牢把握制造业这一立国之本，突出质量这一关键内核，把“质量强国”作为制造业转型升级、实现跨跃发展的战略选择和必由之路。

质量是建设制造强国的生命线。作为未来 10 年引领制造强国建设的行动指南和未来 30 年实现制造强国梦想的纲领性文件，《中国制造 2025》将“质量为先”列为重要的基本指导方针之一。在制造强国建设的伟大进程中，必须全面夯实产品质量基础，不断提升质量品牌价值和“中国制造”综合竞争力，坚定不移地走以质取胜的发展道路。

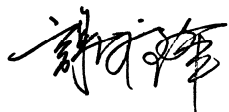
高质量是先进技术和优质管理高度集成的结果。提升制造业产品质量，要坚持从源头抓起，在产品的设计、定型、制造的全过程中按照先进的质量管理标准和技术要求去实施。可靠性是产品性能随时间的保持能力。作为衡量产品质量的重要指标，可靠性管理也充分体现了现代质量管理的特点。《中国制造 2025》提出要加强可靠性设计、试验与验证技术开发应用，使产品的性能稳定性、质量可靠性、环境适应性、使用寿命等指标达到国际同类产品先进水平，就是要将可靠性技术作为核心应用于质量设计、控制和质量管理，在产品全寿命周期各阶段，实施可靠性系统工程。

工业和信息化部电子第五研究所是国内最早从事电子产品质量与可靠性研究的权威机构，在我国的质量可靠性领域开创了许多个“唯一”和“第一”：唯一一个专业从事质量可靠性研究的技术机构；开展了国内第一次可靠性培训；研制了国内第一套环境试验设备；第一个将质量“认证”概念引入中国；建立起国内第一个可靠性数据交换网；发布了国内第一个可靠性预计标准；研发出第一个国际先进、国内领先水平的可靠性、维修性、保障性工程软件和综合保障软件……五所始终站在可靠性技术发展的前沿。随着质量强国战略的实施，可靠性工作在我国得到空前的重视，在新时期的作用日益凸显。五所的科研工作者们深深感到，应系统地梳理可靠性技术的要素、方法和途径，全面呈现该领域的最新发展成果，使之广泛应用于工程实践，并在制造强国和质量强国建设中发挥应有作用。鉴于此，五所在建所 60 周年之际，组织专家学者编写出版了这套“可靠性技术丛书”。这既是历史的责任，又是现实的需要，具有重要意义。

“可靠性技术丛书”内容翔实，涉及面广，实用性强。它涵盖了可靠性的设计、工艺、管理，以及设计生产中的可靠性试验等各个技术环节，系统地论述了提升或

保证产品可靠性的专业知识，可在可靠性基础理论、设计改进、物料优选、生产制造、试验分析等方面为产品设计、开发、生产、试验及质量管理等从业者提供重要的技术参考。

质量发展依赖持续不断的技术创新和管理进步。以高可靠、长寿命为核心的高质量是科技创新、管理能力、劳动者素质等因素的综合集成。在举国上下深入实施制造强国战略之际，希望该丛书的出版能够广泛传播先进的可靠性技术与管理方法，大力推动可靠性技术进步及实践应用，积极推进专业人才队伍建设。帮助广大的科技工作者和工程技术人员，为我国先进制造业发展，落实好《中国制造 2025》发展战略，在新中国成立 100 周年时建成世界一流制造强国贡献力量！

A handwritten signature in black ink, appearing to read '谢辉' (Xie Hui), located in the lower right quadrant of the page.

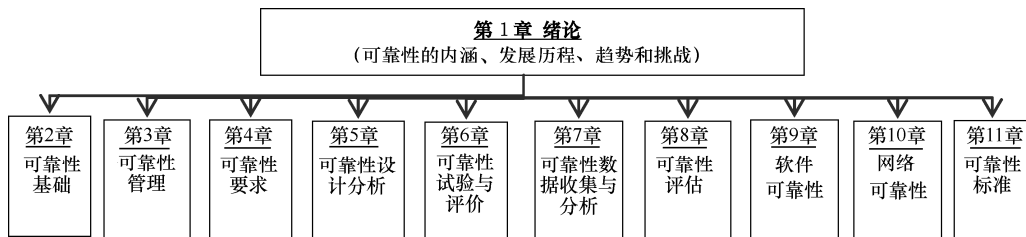
前言

《《《《 PREFACE

本书是工业和信息化部电子第五研究所建所 60 周年献礼可靠性丛书的首册。本书阐述了国内外可靠性工程的发展历程、趋势和面临的挑战，阐明了可靠性工程的作用和主要工作内容，介绍了可靠性的内涵和相关基础知识，并从产品全寿命周期可靠性系统工程的角度，对可靠性管理、技术和标准化等方面进行了概要性的论述。重点阐述了可靠性基础理论、可靠性管理、可靠性建模、可靠性数据收集与处理、可靠性试验评价等基础性的技术和方法。

编者力图通过本书展示可靠性工程的概貌，兼顾理论性和工程实用性，在介绍可靠性基础理论的同时，结合编者多年的可靠性实践经验，给出具体的工程方法和实践案例。

本书内容围绕可靠性工程的主要工作展开，全书共 11 章，其架构如下图所示。对各章内容的编排如下。



第 1 章绪论，概括介绍可靠性的概念与作用、可靠性工程的主要工作内容、发展历程，重点阐述了可靠性工程在复杂系统、信息-物理融合系统、云计算系统、预测与健康管理等、无铅焊点、质量特性综合等方面的发展趋势、面临的挑战 and 对策。

第 2 章介绍可靠性基础，阐述与可靠性相关的条件、时间、功能和能力 4 个要素，失效及其分类，可靠性参数，以及产品的寿命分布函数。

第 3 章介绍可靠性管理的概念、内容和特点，包括可靠性计划、管理组织机构、过程管理、评审和可靠性信息管理等。

第 4 章介绍可靠性要求及其确定的相关过程和技术。

第 5 章介绍可靠性设计分析技术，包括可靠性设计分析的目的和一般原则，可靠

性模型、预计、分配、仿真和分析技术，以及机械可靠性、元器件选用控制等。

第 6 章介绍可靠性试验与评价技术，包括可靠性试验的目的、分类、要素、要求和一般程序，试验类型覆盖可靠性测定试验、验证试验、增长试验、加速试验和与可靠性相关的筛选技术等，并给出了试验评价的模型和方法。

第 7 章介绍可靠性数据收集、处理和分析方法，重点阐述了可靠性数据收集的原理、内容和方法，以及统计分析、分布检验和参数估计方法。

第 8 章介绍可靠性评估的一般程序和方法。本章尤其适用于小子样或大型复杂系统的可靠性评价。在系统研制和使用阶段，进行可靠性评估可有效估计系统的可靠性水平。

第 9、10 章探讨软件和网络可靠性。由于软件和网络的可可靠性与传统的硬件系统可靠性差别很大，其可靠性理论和方法也有很大差异，并且随着软件和网络应用的不断深入，由于它们的失效引发的系统失效占比不断增大，非常有必要辟出专门的章节讨论，深入探讨软件和网络的可可靠性问题。

第 11 章介绍可靠性标准。详细介绍了国内/国际相关的可靠性标准化组织情况，给出了相关标准体系架构和常用的可靠性标准，以方便读者查阅。

其中，第 1 章由潘勇、黄进永、杨洪旗编写，第 2 章由黄进永、张增照编写，第 3、4 章由胡宁、潘勇编写，第 5 章由冯燕宽、黄进永、张增照、黄智伟、周军连、任艳、方子豪、张三娣编写，第 6 章由胡宁、张增照、潘勇编写，第 7 章由葛智君、潘勇编写，第 8 章由黄进永编写，第 9 章由陈冰泉、杨洪旗编写，第 10 章由杨洪旗、黄进永编写，第 11 章由杨洪旗、潘勇编写，全书由潘勇统稿。

本书内容跨度较大，在编写过程中，参阅了前辈和同行编写、提供的大量相关文献资料，并引用了部分内容，在此表示衷心感谢。

张剑伟、朱启新等同事参与了本书部分章节的编写、校对和图表制作等工作，在此谨致感谢。特别感谢莫郁薇研究员对本书提出的宝贵意见。

由于本书编写时间紧迫，成书略显仓促，编者水平所限，错漏之处难免，敬请广大读者批评指正。

编者

2015 年 6 月

目录

<<<<< CONTENTS

第 1 章 绪论	(1)
1.1 可靠性的内涵	(1)
1.2 可靠性的作用和地位	(5)
1.3 可靠性工程的基本内容和特点	(7)
1.3.1 可靠性工程的基本内容	(7)
1.3.2 可靠性工程的特点	(10)
1.4 可靠性工程的发展历程	(11)
1.4.1 概述	(11)
1.4.2 概念形成阶段	(12)
1.4.3 建立阶段	(13)
1.4.4 全面发展阶段	(14)
1.4.5 趋于成熟阶段	(16)
1.4.6 深入发展阶段	(21)
1.5 可靠性工程的发展趋势和面临的挑战	(26)
1.5.1 概述	(26)
1.5.2 复杂系统的可靠性	(27)
1.5.3 动态系统的可靠性	(31)
1.5.4 体系的可靠性	(34)
1.5.5 软硬件综合系统的可靠性	(36)
1.5.6 信息-物理融合系统的可靠性	(39)
1.5.7 云计算系统的可靠性	(41)
1.5.8 可靠性与其他质量特性的综合	(47)
1.5.9 基于失效物理的故障预测与健康管理	(52)
1.5.10 无铅焊点的可靠性	(58)
1.5.11 纳米技术的可靠性	(61)
1.5.12 可靠性仿真试验	(62)
1.5.13 高加速极限试验和应力筛选	(67)
参考文献	(72)

第 2 章 可靠性基础 (75)

2.1 对可靠性定义的进一步理解 (75)

2.1.1 可靠性的构成要素 (75)

2.1.2 规定的任务和功能 (76)

2.1.3 规定的环境和使用条件 (76)

2.1.4 规定的时间 (77)

2.1.5 规定的能力 (79)

2.2 产品的可靠性参数 (82)

2.2.1 常用的可靠性参数 (82)

2.2.2 产品的寿命特征量 (86)

2.2.3 可靠性参数间的相互关系 (89)

2.3 产品的寿命分布 (91)

2.3.1 指数分布 (92)

2.3.2 正态分布 (93)

2.3.3 对数正态分布 (94)

2.3.4 威布尔分布 (95)

2.3.5 超几何分布 (97)

2.3.6 伽马(Γ)分布 (98)

2.3.7 贝塔分布 (99)

2.3.8 寿命分布 (100)

参考文献 (101)

第 3 章 可靠性管理 (102)

3.1 可靠性管理概述 (102)

3.1.1 可靠性管理的概念 (102)

3.1.2 可靠性管理的基本职能 (103)

3.1.3 可靠性管理的基本原则 (104)

3.1.4 可靠性管理的内容 (104)

3.1.5 可靠性管理与质量管理的关系 (106)

3.2 可靠性计划与可靠性工作计划的制订 (108)

3.2.1 目的与作用 (108)

3.2.2 计划的主要内容 (109)

3.2.3 编制可靠性计划与工作计划的一般要求 (110)

3.3 可靠性管理组织 (111)

3.3.1 研制、生产单位的可靠性管理组织 (112)

3.3.2 型号武器系统的可靠性管理组织 (113)

3.4	可靠性过程管理	(115)
3.4.1	研制阶段的可靠性管理	(115)
3.4.2	生产阶段的可靠性管理	(119)
3.4.3	使用阶段的可靠性管理	(120)
3.4.4	对转承制方和供应方的监督与控制	(120)
3.5	可靠性评审	(121)
3.5.1	可靠性评审的作用	(121)
3.5.2	评审组织及程序	(121)
3.5.3	可靠性评审	(122)
3.5.4	软件可靠性设计评审	(125)
3.6	可靠性信息管理	(126)
3.6.1	可靠性信息的分类	(126)
3.6.2	可靠性信息管理工作内容	(129)
3.7	故障报告、分析和纠正措施系统	(132)
3.7.1	概述	(132)
3.7.2	FRACAS 系统的建立	(133)
3.7.3	FRACAS 的运行	(136)
	参考文献	(139)
第 4 章	可靠性要求	(140)
4.1	确定可靠性要求的重要性	(140)
4.2	可靠性要求的表述形式	(140)
4.3	与可靠性要求相关的若干概念和参数	(141)
4.4	可靠性要求	(143)
4.4.1	可靠性定性要求	(143)
4.4.2	可靠性定量要求	(144)
4.5	确定可靠性要求的一般原则和实施要点	(147)
4.6	确定可靠性要求及其验证的一般程序和方法	(152)
	参考文献	(156)
第 5 章	可靠性设计分析	(158)
5.1	可靠性设计分析概述	(158)
5.1.1	目的	(158)
5.1.2	一般程序和主要方法	(160)
5.1.3	可靠性设计准则	(162)
5.2	指导思想和原则	(166)
5.3	可靠性建模	(170)

5.3.1	可靠性模型的内涵和作用	(170)
5.3.2	基本可靠性模型	(170)
5.3.3	任务可靠性模型	(172)
5.3.4	基本可靠性与任务可靠性的区别和联系	(173)
5.3.5	基本可靠性和任务可靠性的权衡	(173)
5.3.6	建立可靠性模型的一般程序	(174)
5.3.7	典型的系统可靠性模型	(179)
5.3.8	共因故障模型	(188)
5.3.9	多功能系统模型	(190)
5.3.10	储存可靠性模型	(191)
5.4	可靠性分配	(193)
5.4.1	可靠性分配的目的和作用	(193)
5.4.2	可靠性分配考虑的因素	(193)
5.4.3	可靠性分配的原理和准则	(194)
5.4.4	可靠性分配的参数	(195)
5.4.5	可靠性分配的层次	(195)
5.4.6	可靠性分配的方法	(196)
5.4.7	不同研制阶段可靠性分配方法的选择	(202)
5.4.8	进行可靠性分配时的注意事项	(202)
5.5	可靠性预计	(203)
5.5.1	可靠性预计的目的和作用	(203)
5.5.2	可靠性预计的内容	(205)
5.5.3	系统可靠性预计方法	(205)
5.5.4	主要的可靠性预计标准及其发展状况	(214)
5.5.5	进行可靠性预计时的注意事项	(220)
5.6	可靠性仿真	(221)
5.6.1	可靠性仿真的内涵、条件和优势	(221)
5.6.2	可靠性仿真的一般流程	(223)
5.6.3	可靠性仿真的技术难点	(224)
5.7	故障模式、影响及危害性分析 (FMECA)	(224)
5.7.1	FMECA 的方法概述	(224)
5.7.2	FMECA 的作用	(226)
5.7.3	FMECA 的实施要求和注意事项	(229)
5.7.4	FMECA 的工作内容和一般步骤	(231)
5.7.5	FMECA 相关技术标准状况	(237)

5.8 故障树分析..... (242)

5.8.1 故障树分析概念..... (242)

5.8.2 FTA 发展及应用..... (243)

5.8.3 FTA 中的图形符号..... (244)

5.8.4 故障树分析的一般方法与流程..... (247)

5.8.5 共因故障问题..... (255)

5.8.6 动态故障树分析..... (255)

5.9 潜在通路分析..... (257)

5.9.1 潜在通路分析的内涵..... (257)

5.9.2 潜在通路的特点..... (257)

5.9.3 潜在通路产生的原因..... (258)

5.9.4 潜在通路的表现形式..... (258)

5.9.5 潜在通路分析技术现状..... (259)

5.9.6 潜在通路分析方法与流程..... (260)

5.10 电路容差分析..... (265)

5.10.1 容差分析的内涵..... (265)

5.10.2 容差分析程序..... (266)

5.10.3 容差分析方法..... (267)

5.10.4 容差分析实施要点..... (268)

5.10.5 使用软件工具进行容差分析示例..... (269)

5.11 耐久性分析..... (270)

5.11.1 目的..... (270)

5.11.2 一般信息..... (270)

5.11.3 耐久性分析程序..... (270)

5.12 失效物理分析..... (271)

5.12.1 概述..... (271)

5.12.2 失效物理模型示例..... (272)

5.12.3 失效物理分析法应用示例..... (275)

5.13 机械可靠性..... (278)

5.13.1 机械可靠性现状..... (278)

5.13.2 机械可靠性特点..... (279)

5.13.3 结构可靠性分析..... (280)

5.13.4 机构可靠性分析..... (281)

5.14 元器件的选用控制..... (282)

5.14.1 选用的必要性..... (282)

5.14.2	元器件选用管理的内容	(282)
5.14.3	优选管理	(288)
5.14.4	质量控制	(290)
参考文献		(294)
第 6 章	可靠性试验与评价	(295)
6.1	概述	(295)
6.1.1	可靠性试验的目的	(295)
6.1.2	可靠性试验的分类及其主要用途	(296)
6.1.3	可靠性试验的要素	(302)
6.1.4	可靠性试验的计划与要求	(306)
6.1.5	可靠性试验方案及一般程序	(309)
6.2	可靠性测定试验和可靠性增长测定试验	(312)
6.2.1	可靠性测定试验	(312)
6.2.2	可靠性增长测定试验	(315)
6.3	可靠性验证试验	(320)
6.3.1	抽样检验	(320)
6.3.2	可靠性验证试验大纲要求	(324)
6.3.3	平均寿命抽样检验的原理与试验方案	(326)
6.4	环境应力筛选 (ESS)	(330)
6.4.1	环境应力筛选的目的	(330)
6.4.2	环境应力筛选的原理	(330)
6.4.3	试验剖面的确定	(331)
6.4.4	典型的环境应力筛选过程	(333)
6.5	可靠性增长试验	(336)
6.5.1	可靠性增长试验的内涵及其作用	(336)
6.5.2	可靠性增长试验的时机	(337)
6.5.3	可靠性增长试验方法	(337)
6.5.4	常用可靠性增长模型	(339)
6.5.5	可靠性增长试验计划曲线	(342)
6.5.6	可靠性增长试验的跟踪与控制	(345)
6.5.7	可靠性增长试验的最终评定	(346)
6.6	加速试验	(346)
6.6.1	加速试验的目的和基本原理	(346)
6.6.2	加速寿命试验	(349)
6.6.3	高加速极限试验和应力筛选试验	(354)

6.6.4	加速试验的局限性	(372)
	参考文献	(373)
第 7 章	可靠性数据收集与分析	(374)
7.1	概述	(374)
7.1.1	数据、信息的概念及特征	(374)
7.1.2	数据的收集与分析	(377)
7.2	可靠性数据的重要性	(378)
7.3	可靠性数据收集与分析的基本要求	(379)
7.3.1	可靠性数据收集的目的	(380)
7.3.2	可靠性数据收集的要求及注意事项	(381)
7.3.3	可靠性数据分析的目的和任务	(383)
7.3.4	可靠性数据分析的要求和注意事项	(383)
7.4	可靠性数据收集	(384)
7.4.1	可靠性数据的分类	(384)
7.4.2	可靠性数据的内容	(386)
7.4.3	可靠性数据收集的原理	(389)
7.4.4	可靠性数据收集的方式	(395)
7.4.5	可靠性数据收集的程序和方法	(397)
7.5	可靠性数据处理与统计分析概述	(400)
7.6	可靠性数据的初步处理	(403)
7.6.1	数据的集中性和分散性	(404)
7.6.2	样本的频率分布	(407)
7.6.3	周期测量数据的统计处理	(410)
7.6.4	散布图	(411)
7.6.5	回归分析	(414)
7.6.6	方差分析	(416)
7.7	可靠性数据分析的数学方法	(418)
7.7.1	分布类型检验	(418)
7.7.2	分布参数估计	(430)
7.7.3	贝叶斯方法在可靠性数据分析中的应用	(446)
7.8	可靠性数据库	(447)
7.8.1	概述	(447)
7.8.2	GIDEP	(447)
7.8.3	IHS	(450)
7.8.4	RIAC	(451)

7.8.5	美国的核电可靠性数据系统 (NPRDS)	(452)
7.8.6	CEPREI_RDC	(453)
	参考文献	(455)
第 8 章	可靠性评估	(457)
8.1	可靠性评估的作用	(457)
8.2	可靠性评估的工作内容和程序	(458)
8.3	可靠性评估的数据收集和处理	(462)
8.3.1	可靠性评估数据的收集	(462)
8.3.2	可靠性评估数据的处理	(463)
8.4	设备的可靠性评估方法	(466)
8.4.1	成败型设备的可靠性评估	(466)
8.4.2	指数寿命型数据可靠性评估	(467)
8.5	基于经典法的复杂系统可靠性评估	(469)
8.5.1	成败型 (二项分布) 串联系统可靠性评估	(469)
8.5.2	二项分布单元并联系统的可靠性评估	(471)
8.5.3	寿命型 (指数分布) 单元串联系统的可靠性评估	(471)
8.5.4	指数分布单元并联系统的可靠性评估	(473)
8.6	基于 Bayes 的复杂系统可靠性评估	(473)
8.6.1	由指数寿命型单元组成的系统可靠度	(473)
8.6.2	串联系统可靠度	(475)
8.6.3	并联系统可靠度	(476)
8.7	可靠性评估案例	(478)
8.8	可靠性评估注意事项	(478)
	参考文献	(479)
第 9 章	软件可靠性	(480)
9.1	引言	(480)
9.2	基本定义和术语	(481)
9.2.1	软件的定义	(481)
9.2.2	软件可靠性的相关术语	(481)
9.3	软件故障的分类	(482)
9.4	软件可靠性与硬件可靠性	(483)
9.4.1	软件可靠性与硬件可靠性之间的区别	(483)
9.4.2	软件可靠性与硬件可靠性之间的相似之处	(485)
9.5	软件可靠性统计模型	(485)
9.5.1	主要统计模型	(485)

9.5.2	模型评价	(493)
9.6	软件可靠性设计	(495)
9.7	软件可靠性分配	(498)
9.7.1	考虑因素	(498)
9.7.2	基本公式	(500)
9.8	软件可靠性预计	(500)
9.8.1	基于模型的软件可靠性预计	(501)
9.8.2	基于经验公式的软件可靠性预计	(504)
	参考文献	(509)
第 10 章	网络可靠性	(511)
10.1	引言	(511)
10.2	网络理论的发展历程和相关概念	(512)
10.2.1	网络理论的发展历程	(512)
10.2.2	网络的概念和特征量	(514)
10.2.3	网络的分类	(517)
10.3	网络可靠性发展历程及相关概念	(519)
10.3.1	网络可靠性研究的历程	(519)
10.3.2	网络及可靠性的相关术语	(523)
10.3.3	网络可靠性定义	(524)
10.3.4	网络故障的来源	(525)
10.3.5	网络故障的分类	(525)
10.4	网络可靠性研究的理论方法	(527)
10.5	网络可靠性度量参数体系	(528)
10.5.1	建立原则	(528)
10.5.2	网络可靠性的通用参数体系	(528)
10.5.3	通信网络可信性参数体系	(530)
10.6	网络可靠性建模	(536)
10.6.1	网络可靠性建模的实施要点	(537)
10.6.2	网络可靠性模型分类	(537)
10.6.3	基于排队论的可靠性模型	(538)
10.6.4	马尔可夫链模型	(539)
10.6.5	考虑加权因子的可靠性模型	(543)
10.6.6	基于 Petri 网的可靠性模型	(545)
10.6.7	基于信息动力学的网络性能可靠性模型	(545)
10.6.8	交通网行程时间可靠性模型	(548)

10.6.9	相继故障传播模型	(548)
10.7	网络可靠性计算	(549)
10.7.1	解析算法	(550)
10.7.2	仿真算法	(550)
10.7.3	网络可靠性计算方法比较	(551)
10.8	网络可靠性评估	(553)
10.8.1	可靠性评估方法概述	(553)
10.8.2	连通可靠性评估	(554)
10.8.3	容量可靠性评估	(555)
10.8.4	性能可靠性评估	(556)
10.8.5	以业务为中心的网络可靠性综合评估	(557)
10.9	网络可靠性设计	(558)
10.9.1	可靠性设计概述	(558)
10.9.2	通信网可靠性设计准则	(563)
10.10	网络可靠性管理	(564)
10.11	小结	(566)
	参考文献	(566)
第 11 章	可靠性标准	(570)
11.1	概述	(570)
11.2	可靠性国际标准	(571)
11.2.1	可靠性国际标准组织	(571)
11.2.2	IEC 制定的可靠性标准	(571)
11.2.3	ISO 制定的可靠性标准	(579)
11.2.4	IEEE 制定的可靠性标准	(582)
11.3	可靠性国家标准/国家军用标准	(583)
11.3.1	可靠性国家标准	(583)
11.3.2	可靠性国家军用标准	(586)
11.4	美国军用可靠性标准	(591)
11.5	可靠性行业标准	(594)
11.5.1	核电可靠性标准	(594)
11.5.2	电力可靠性标准	(594)
11.5.3	汽车可靠性标准	(595)
11.5.4	航天可靠性标准	(597)
11.5.5	航空可靠性标准	(598)
	参考文献	(599)

第1章

绪论

1.1 可靠性的内涵

在日常生活中，我们经常会谈论到产品的质量、可靠性和寿命这些概念，它们的内涵和范畴如何？有什么区别和联系？

在本书的开篇，首先明确与质量、可靠性相关的几个概念。

先来分享两个真实的故事。也许，它们对读者理解这些概念会有帮助。

进入 21 世纪，移动互联网飞速发展，正在改变人类的生活和思维方式，而移动通信基站是移动互联网的核心基础设施之一。将要讲述的两个故事都与公用移动通信基站有关。公用移动通信基站是无线电台（站）的一种形式，是指在一定的无线电覆盖区中，通过移动通信交换中心，与移动电话终端之间进行信息传递的无线收发电台。

第一个故事是关于 2008 年北京奥运会圣火传递的。据中国移动网站发布消息：2008 年 5 月 8 日，设置在珠穆朗玛峰（以下简称“珠峰”）5200 米和 6500 米处的基站，出色完成了北京奥运圣火登顶珠峰的通信保障任务。珠峰的自然环境对通信设备是一个极其严峻的考验。珠峰不可能提供常规维护条件，移动基站设备必须达到超常规的稳定性和零故障，以保证通信网络的稳定、可靠运行。由于零故障和持续稳定的工作，珠峰移动网络实现了基站设备的“零值守”，不需要现场维护。

请注意上述故事中的“可靠”、“珠峰的自然环境”、“通信”、“零故障和持续稳定的工作”等术语，这些正是本书将要论述的可靠性的关键要素。

由此引出可靠性的定义：产品在规定的条件下和规定的时间内，完成规定功能的能力，其概率称为可靠度。

注意定义中的 3 个“规定”，它们正是可靠性的 4 个要素中的 3 个（另一个要素为“能力”）。

这个定义对应到上述故事中，产品就是公用移动通信基站；3 个要素分别是：

规定的条件是指其工作的珠峰风急高寒等恶劣自然环境下的运行条件，规定时间是北京奥运会圣火在珠穆朗玛峰传递历经的时间，规定的功能是基站正常收发信息，以便保障在珠峰能正常通信。

故事中的“零故障和持续稳定的工作”，即要求圣火在珠峰传递期间，通信不能出现任何故障，即可靠度达到 100%。

第二个故事是关于开拓海外市场的。

近年来，当众多的国内电子产品制造商正在历经返修率居高不下、产品利润无法保证、品牌形象受损的痛苦煎熬时，作为中国通信行业代表性企业的某电信公司，却能从容应对通信网络技术的快速演进，凭借其推出的第 4 代基站在海外攻城略地，一路攻克欧洲著名的跨国电信运营商 O₂ 在德国、捷克、西班牙的机构，以及捷克的另一移动通信巨头 T-Mobile 等，甚至还包括新加坡 M1、孟加拉国 GrameenPhone 等全球运营商，从欧洲席卷全球。那么，究竟是什么让该电信公司在与众多的老牌电信运营商之间的竞争中从容胜出的？

也许读者会说是该电信公司决策层走出去的决心，或者说是其海外市场营销人员努力的结果。没错，这些都是重要因素。但是，国内不乏豪情万丈声称要走出去的大腕，并且通过并购国外公司获取了现成的营销网络，为何大多铩羽而归？还是听听客户是怎么说的吧！

- 德国 O₂ 的首席技术官（CTO）Andrea Folgueiras 先生说：“该电信公司的解决方案非常先进，这对 O₂ 很重要。O₂ 最看重的是该电信公司解决方案的融合能力，能够将 GSM 和 UMTS 的模块集成到一个基站内，这使得 O₂ 部署的 GSM 基站随时能够轻松升级到 UMTS，并降低了运维成本。”
- 西班牙电信和 O₂ 驻捷克的董事局主席 Salvador Anglada 先生说：“选择该电信公司，因为其拥有丰富的经验和高质量的产品，并且在技术上非常成熟。”
- T-Mobile 捷克的执行副总裁 Heinz Schmid 先生解释说：“该电信公司的新设备将使网络性能大大提升，并能使我们给用户提供更多、更新的业务，例如高速数据业务。整个网络都将拥有更先进的性能。”

从他们的言谈中可以看出，选择该电信公司产品的根本原因在于，该电信公司的产品能够满足他们的需求目标。请注意他们提到的“能力”、“运维成本”、“高质量”、“性能”这些词，由此引出质量特性的定义。

根据 GB/T 19000-2008/ISO 9000:2005《质量管理体系基础和术语》第 3.5.2 节中的定义，质量特性（Quality Characteristic）是指与要求有关的产品、过程或体系的固有特性。质量特性包括性能、寿命、实用性、可信性、易用性、经济性和美观等属性。

下面以产品为例，介绍其主要质量特性。

1. 性能 (performance)

性能通常是指产品在功能上满足顾客要求的能力。以移动电话为例，其主要性能包括 CPU 频率、显示器分辨率、电池续航时间等。

2. 可信性 (dependability)

可信性可理解为广义的可靠性。根据 IEC 60050-192:2015《电工术语 可信性》第192-01-22条的定义，可信性是指产品需要时按要求执行的能力。它是产品与时间相关质量特性的集合，包括可用性、可靠性、恢复性、维修性和保障性，在某些情况下还包括诸如环境适应性、耐久性、安全性和信息安全等其他特性。而根据总装备部 2014 年 5 月 8 日颁布的《装备通用质量特性管理工作规定》中的定义，通用质量特性主要是指可靠性、维修性、保障性、测试性、安全性和环境适应性等质量特性。可见，可信性与国内通常说的通用质量特性大体上同义。

可靠性反映产品在规定的运行环境下和规定的时间内完成规定的功能不出现故障的能力。可靠性是产品固有的设计特性，作为在使用和保障成本、系统效能方面的主要影响因素，在系统费效关系中起到关键作用。而可靠性工程是为确定和达到产品的可靠性要求所进行的一系列技术与管理活动，包括可靠性论证、分析设计、试验评价、使用保障和综合管理等。

经常使用到的与可靠性密切相关的概念还有耐久性 (durability) 和寿命 (lifetime)。耐久性是指产品在规定的使用、储存与维修条件下，达到极限状态之前，完成规定功能的能力，一般用寿命表示。这里，极限状态是指由于耗损（如疲劳、磨损、腐蚀、变质等）使产品从技术上或从经济上考虑，都不宜再继续使用而必须大修或报废的状态。寿命是指产品能够正常使用的年限，包括使用寿命和储存寿命两种。使用寿命是指产品在规定的使用条件下完成规定功能的工作总时间。一般地，不同的产品对使用寿命有不同的要求。储存寿命是指在规定储存条件下，产品从开始储存到规定失效的时间。

可靠性指标主要取决于设计，同时与使用、管理和维修等因素有关。可靠性反映了产品是否容易发生故障的特性，其中基本可靠性反映了装备故障引起的维修保障资源需求，任务可靠性反映了产品功能特性的持续能力。

以下简要介绍几个与可信性相关的概念。注意，在后续广义可靠性的讨论中，还会谈及它们。

- 维修性 (maintainability) 是指产品在规定的条件下和规定的时间内，按规定的程序和方法进行维修时，保持或恢复到规定状态的能力。维修性反映产品



修理的难易程度，一般用平均修复时间、拆装时间、维修工时等来度量。

- 保障性 (supportability) 对军用装备而言，是指装备的设计特性和计划的保障资源满足平时战备完好性和战时利用率要求的能力。保障性描述的是装备使用和维修过程中保障是否及时的能力。而对民用装备而言，是指装备的设计特性和计划的保障资源满足装备维修保障要求的能力。保障性一般用平均保障延误时间、资源满足率、资源利用率等参数来度量。
- 测试性 (testability) 是指产品能及时并准确地确定其状态 (可工作、不可工作或性能下降)，并隔离其内部故障的能力。测试性反映产品是否易于测试、出现故障时是否易于检测和隔离，一般用检测时间、技术准备时间、故障检测率、故障隔离率等参数来度量。
- 安全性 (safety) 是指产品所具有的不导致人员伤亡、系统毁坏、重大财产损失或不危及人员健康和环境的能力。安全性可理解为产品在任何情况下对人员、系统、财产和环境都不构成安全威胁。它可定义为产品在规定的条件下和规定的时间内，以可接受的风险执行规定功能的能力。安全性一般用事故概率、损失率、安全可靠度等参数来度量。
- 环境适应性 (environmental worthiness) 是指产品在其寿命期内预计可能遇到的各种环境作用下能实现其所有预定功能、性能和 (或) 不被破坏的能力。它反映了产品对各种环境的适应能力，即在其可能遇到的各种环境下均能正常工作的能力，是可靠性的一种特殊情况。

现代社会，人类比以往任何时候都更加关注产品的质量，而可信性是产品质量特性的核心属性之一。可信性是产品最为重要的质量指标之一，显然，可信性好的产品，必然是一个可用，而且好用的产品。

3. 经济性

经济性是指产品寿命周期的费用，包括生产、销售过程的费用和使用过程的费用。经济性是保证组织在竞争中得以生存的关键特性之一，是用户日益关心的一个质量指标。价廉物美实际上是反映人们的价值取向，物有所值，就是表明质量有经济性。

经济承受性 (affordability) 是指用户在产品的寿命周期内，能够承担产品研制、采购、使用和保障费用的能力。它是产品设计中考虑使用和保障费用与研制和制造费用的权衡结果。

为帮助读者更直观地理解质量特性、可信性、可靠性的内涵和范畴，图 1-1 给出了它们之间关系的示意图。

可靠性是产品质量特性中最为基础、最为重要的特性，本书将以可靠性为主

题，围绕可靠性工程展开。

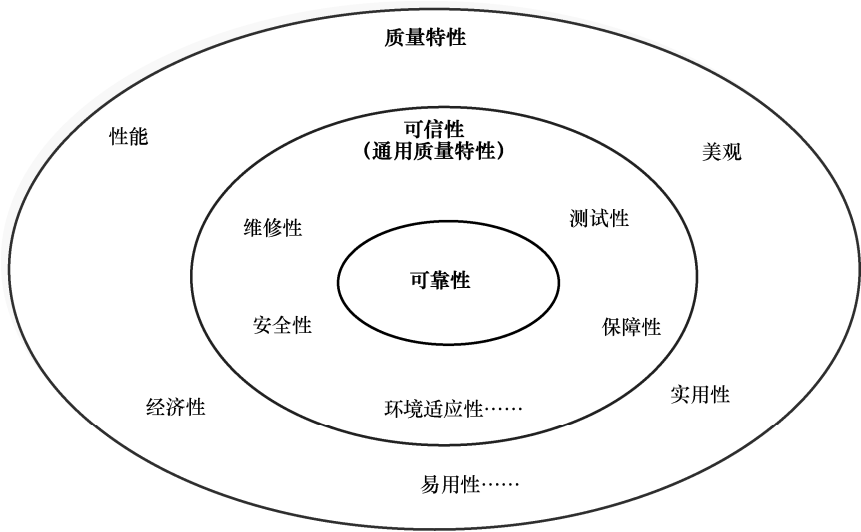


图 1-1 质量特性、可信性与可靠性的范畴示意图

1.2 可靠性的作用和地位

可靠性诞生于 20 世纪 40 年代末，至今已有 70 多年的历史。然而，一直以来，很多机构和个人对于可靠性工作的作用和意义不是很了解，仍然存在认识上的偏差，搞不清楚开展可靠性工作到底有什么作用、能够达到怎样的效果，甚至认为产品搞出来后性能合格就行，可靠性工作只是一种形式，做与不做都一样。这是因为，他们认识不到可靠性是产品核心竞争力之一，而提高产品的可靠性是一项系统性的、基础性的工作，需要不断积累、持续改进，长期保持，才能见成效。不是说今天开展了可靠性工作，明天产品的可靠性就能显著提升了。

开展可靠性工作的主要作用和地位主要表现在如下几个方面。

1. 降低产品失效率和产品寿命周期费用

可靠性工作是一项与故障（或失效）作斗争的工作，开展可靠性工作最基本的作用是降低产品的失效率，节省产品的寿命周期费用。可靠性差的产品，意味着高返修率，由此带来的昂贵维修费用及生产厂家声誉上的损失，是任何一个企业都不希望发生的。但是，要降低产品的失效率，需要相应的技术、经济投入保障，必然会带来产品研制费用的增加。但是，研制出来的产品可靠性提高了，产品在使用阶段的维修保障费用会显著下降。因此，开展可靠性工作的另一个作用是找到产品失效率与总费用的平衡点（可承受费用），根据这个平衡点进行产品的研制和使用维

护决策。图 1-2 是产品寿命周期费用与可靠性的关系示意图。

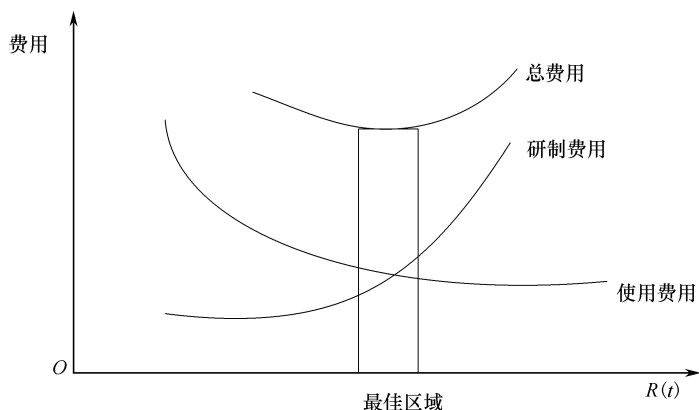


图 1-2 寿命周期费用与可靠性的关系

2. 可靠性工程是高可靠产品的保证

随着工业技术的发展，产品或系统日益向大型化、复杂化或微观化等方向发展，尤其是工业与信息技术的融合发展，整机、系统变得庞大、复杂，构成的零部件、软件数量日益增加，从而使整机、系统发生故障的概率显著增加。例如，汽车中的转向机构，原来采用摇臂、拉杆和蜗杆传动的机械式机构仅需十几个零件，发展为高效的电液式转向机构以后，组成的零件增至近 200 个。同样是实现转向功能，后者的故障机会显然增加。许多机电设备的构成零部件多达上万个，阿波罗宇宙飞船总共使用了 7 100 000 多个元器件，任一元器件的失效都有可能导导致整机或系统的故障，因此为了使整机或系统的可靠性不致下降，必须提高元器件的可靠性水平，同时从整机、系统的设计上予以保证。此外，由于工业技术发展迅速，新材料、新工艺不断涌现，产品更新快，许多新技术等不及试验成熟就投入使用，造成故障不断。纳米材料和器件的应用、大型软硬件结合系统、网络系统、云计算及物联网等的出现，使其可靠性问题变得更为突出。为此，需要有一套保证产品或系统可靠性的工程技术支撑。

3. 社会 and 用户需要高可靠性的产品

随着社会的进步和人们生活水平的不断提高，社会 and 用户对产品的可靠性要求越来越高。随着系统集成度和复杂度的不断提高，因事故或故障引起的人员和财产损失也随之增大，反之，提高装备可靠性的效益也日益显现。例如，1984 年 12 月美国联合碳化物公司设在印度某地的一个农药厂，由于毒气罐阀门失灵造成了上千人死亡、数十万人受到伤害的严重后果；哥伦比亚号航天飞机的爆炸失事更是人类航天史上永久的伤痛；2000 年悉尼夏季奥运会“水火交融”虽被全世界观众津津乐

道,但仍经历了4分钟的黑色尴尬:火炬手在水中点燃主火炬之后,主火炬沿着斜坡上升时出现机械故障,在2米的高度停留了4分钟;2010年的温哥华冬奥会开幕式,最终被定格为一个残缺的作品,点火仪式出现故障,与主火炬一起构成点火装置的4根冰柱只升起了3根,另外1根由于液压系统故障无法升起。类似这样的例子很多,可以说是不胜枚举。因此,为了避免不必要的经济损失或社会影响,必须打造高可靠性的产品或系统。

对高可靠性产品的需求和保证甚至上升到了法律层面。为了维护用户权益和社会效益,某些工业国家还实施了产品责任法。自1994年开始,我国也实施了消费者权益保护法,根据这些法律,只要因产品的缺陷或故障对用户造成损失,除了保修期内的索赔外,用户还可以向法庭提起诉讼。

4. 可靠性是产品的核心竞争力

产品竞争是经济发展的必然趋势。能在竞争中取胜,赢得市场的,必然是那些产品质量可靠性过硬、信誉良好的企业。目前国际上的大多数产品,如发电设备、航空器、通信系统等,在投标和签订合同时都需要明确可靠性指标。对于可维修的设备,用户不仅要考虑购置费用,还要考虑使用和维修的费用,即从全寿命周期费用的观点来权衡和选购产品。在产品性能不相上下的情况下,其可靠性就可能成为制胜的法宝。我国若要实现从制造大国向制造强国转型,则产品的质量和可靠性问题是必须逾越的屏障。

5. 产品的可靠性是一个企业乃至国家科技水平的重要标志

很多成功的企业,百年不倒,不断发展壮大。家喻户晓的宝马、奔驰、西门子等顶尖品牌,成为“德国制造”高品质的名片;中国南车和北车集团制造的高铁能够驶出国门、走向世界,除了很高的性价比外,其可靠性和安全性无疑是一大卖点。这些企业无一例外,都非常重视产品的质量和可靠性。早在1969年,美国宇航局就将可靠性工程列为阿波罗飞船登月成功的三大技术成就之一。我国神舟系列飞船和探月工程的成功,其可靠性也是关键要素之一。这些大型工程能安全可靠的成功实施,也在一定程度上反映了一个国家的科技水平。

1.3 可靠性工程的基本内容和特点

1.3.1 可靠性工程的基本内容

从工程视角来看,可靠性工作可理解为使产品能够保持无故障完成规定功能的状态所实施的一系列活动。可靠性工程是指为了确定和达到产品的可靠性要求所进

行的一系列技术与管理活动。可靠性工程涉及产品可靠性要求论证、可靠性设计分析、可靠性试验评价、生产和使用阶段的可靠性评估与改进，以及产品寿命周期可靠性管理等内容。

产品的可靠性工程贯穿产品寿命周期从概念、方案、研制、设计、生产、使用到报废处置各阶段。它涉及原材料、元器件、设备、软件、系统和系统工程等各个方面。造成产品不可靠的因素是多方面的，既有客观上的因素也有主观上的因素，既与技术水平有关也与认识水平及管理水平有关。我国的可靠性工作开展了 50 多年，取得了很大的进步，各领域、各行业对产品可靠性的重要性认识也慢慢提高了。在很多的产品设计、开发过程中，都开展了可靠性工作。但是，要提高产品的可靠性是一项非常艰巨的任务，它不仅需要管理者的重视、技术人员的参与，而且可靠性工作是一项系统工程，需要与实际的产品相结合开展才有意义。也就是说，不同的产品，可能在开展可靠性工作时，会有不同的侧重点，即有所区别。一般而言，可靠性工程包括可靠性管理工作和可靠性技术工作两方面。

为便于读者理解，把可靠性工程的主要工作内容进行梳理，见图 1-3。

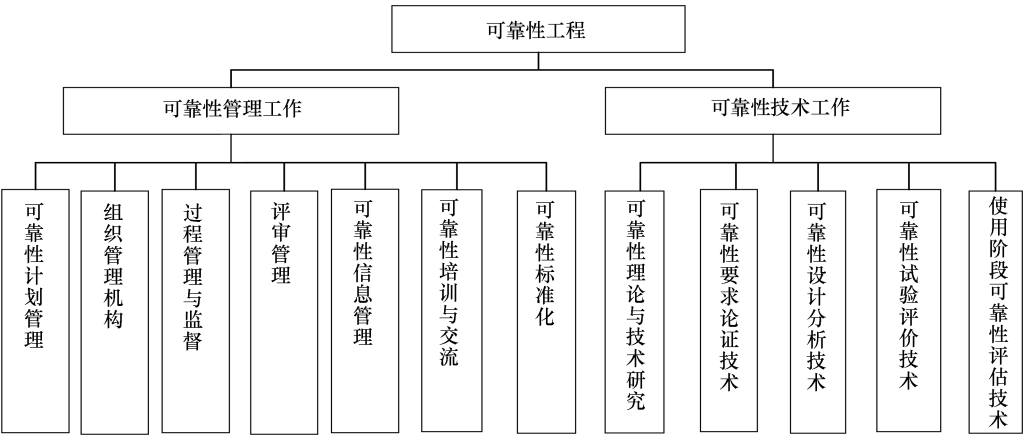


图 1-3 可靠性工程的主要工作示意图

1. 可靠性管理工作

可靠性工作是一项综合性的技术工作，它需要各部门之间的共同努力和密切协作。由谁来组织各部门之间的平衡和协调？由谁来下达可靠性任务？由谁来制订可靠性计划并督促实施？由谁来组织可靠性审查？这些都牵涉到可靠性管理工作。在任何机构里，凡是与可靠性有关的各项措施必须自上而下地贯彻执行，也就是说，可靠性管理，不光是管理人员的工作，应该是全员参与。可靠性管理在可靠性工程中起着决定性的作用。工程上说的“三分技术，七分管理”恰如其分地说明了管理工作的重要性。只有加强可靠性管理，才能提高产品的可靠性。某厂为了给工程上

提供一批高可靠性的元器件，并没有引入什么新的技术装备，只是加强了管理，把技术上过硬的熟练工人调到专用生产线上，并且组织有关人员在每一个关键工序后进行严格的检验，其结果是筛选淘汰率从 10%~20%降低到 1%~3%，达到了较高的可靠性水平。在 20 世纪 80 年代，我国电视机的电、光、声性能指标已接近国际水平，但其可靠性水平（平均故障间隔时间）却只有 500 小时。当时，管理机构明确将可靠性问题列为主攻方向，明确了平均无故障工作时间应达 2000 小时以上的目标，加强了可靠性管理，最终提高了电视机产品的可靠性水平。随着可靠性工程的不断发展，装备的可靠性工作项目越来越多，与其他工作的接口越来越复杂，可靠性管理工作更显其重要性。

可靠性管理范围很广，包括制定可靠性规划、调度为实施该规划所需的人力物力资源，确定实施可靠性规划的体制以及制定可靠性标准规范；开展可靠性教育培训；进行可靠性信息反馈等。几乎企业经营管理的各个方面，诸如人事管理、财务管理、销售管理、器材管理、生产管理、技术计划管理等都可能存在与产品可靠性管理相关的问题。

可靠性管理机构可以分为国家级、行业级和企业级等。

- 国家级可靠性管理机构的主要任务是提出可靠性目标，制定可靠性规划，确定可靠性投资，组织可靠性的分工协调，建立可靠性试验认证机构和失效分析机构，组织可靠性数据交换和信息反馈工作，开展可靠性宣传教育活动，制定可靠性标准，组织可靠性评审，进行技术学术交流，开展可靠性理论研究攻关等。
- 行业级管理机构的主要工作包括制定本行业的可靠性规划，制订行业可靠性标准规范，组织行业内的可靠性活动，促进本行业的可靠性发展等。
- 企业级可靠性管理机构的主要任务是明确企业的可靠性指标，制订可靠性计划，进行可靠性的预计与分配，制定原材料或元器件的采购方针，签订可靠性相关协议，进行可靠性设计，开展可靠性教育和培训，进行可靠性试验，制定信息反馈制度，编制产品使用和维护手册等。

2. 可靠性技术工作

可靠性技术工作包括可靠性论证、分析、设计、试验评价，生产过程的可靠性控制，以及使用和维护阶段的可靠性数据收集、处理和评估等技术工作。可靠性论证的主要目的是合理确定产品可靠性目标和要求。可靠性预测及分析的主要目的是建立系统的可靠性预测模型，并对系统的各组成部分进行可靠性预测和分析，合理预计产品的可靠性水平，找出薄弱环节。可靠性预测及分析的主要方法有可靠性模型分析法、网络分析法、布尔代数法、失效物理分析法、故障树法、蒙特卡洛法、

上下限法、故障模式与影响分析等。可靠性设计的主要方法有冗余性设计、容差设计、容错设计、耐环境设计等。可靠性试验包括环境试验、寿命试验、可靠性验收和鉴定试验、加速试验和环境应力筛选、元器件失效率鉴定试验以及设备平均无故障工作时间的验证试验等。生产过程的可靠性控制的主要手段是对人、机、生产环境、生产材料、生产工艺进行严格的控制,以实现既定的可靠性目标。使用和维护阶段的可靠性技术工作包括确立和优化使用与维护方案、优化备件策略、确定更换办法并建立和健全故障记录制度,以及可靠性数据的收集、处理和评估技术、可靠性增长评估等。收集交换可靠性数据的目的是将来自工厂、用户以及可靠性试验研究机构的各种数据加以归纳、整理和统计分析,尽快地将各种信息反馈到设计生产部门,以促进产品可靠性水平的提高。

可靠性是一个综合性学科,可靠性工程的不断发展,促进了可靠性数学与可靠性物理等理论研究的不断深入。可靠性数学除了必须应用概率论等基本知识外,还需要运用假设检验、参数估计、多元分析、抽样理论、随机过程、小子样理论等有关知识;在可靠性系统分析中,除了必须应用随机事件的和、随机事件的积等基本知识外,还需要用到布尔代数、网络分析、代数学、拓扑学、图论、运筹学、蒙特卡洛法、仿真科学、贝叶斯方法以及系统工程等理论和方法。在可靠性物理中需要研究材料性能、环境应力以及失效物理学等。由于科学技术的不断发展,各种学科互相渗透的现象,在可靠性理论研究中显得尤为突出。

1.3.2 可靠性工程的特点

产品的可靠性指标与产品技术性能指标有着极为密切的联系。

- 一方面,如果没有基本的技术性能指标,产品的可靠性问题就无从谈起。所谓产品的不可靠,是针对产品的某些基本性能而言的。以电视机为例,可以用“完全没有图像”、“完全没有伴音”作为出现故障的标志;也可以用“图像模糊”、“图像跳动”作为出现故障的尺度;还可以用“伴音失真”或者是“图像明亮度、清晰度、失真度、稳定度等方面不符合要求”作为出现故障的判定标准。因此,产品“出现故障”可以有各种各样的形式,也可以有各种各样的判断标准。
- 另一方面,如果产品不可靠,即使其技术性能再好也得不到发挥。对电视机来说,如果频道很多,屏幕很大、图像清晰、伴音优美,但经常出故障,那就会影响收听收看的效果,其优点就得不到发挥。对尖端武器而言,如果它不可靠,那就无法发挥其效能,而且还有可能伤害自己。

产品的可靠性指标,可以针对某些单项技术性能指标而言,也可以针对许多技

术性能指标的综合而言，因此，产品的可靠性指标是一个与许多因素相关的综合性的质量指标。

产品的可靠性，不但有与设计 and 生产有关的所谓“固有可靠性”，而且有与使用条件有关的所谓“使用可靠性”。产品的可靠性要在使用过程中经受时间的考验。家用电器需要做到“经久耐用”；收录机、电视机应该在使用过程中做到“少出毛病”；通信装备在战场中应该“迅速、准确”、“连续不间断”地传递军事信息；导弹核武器在使用过程中应该“稳妥可靠、万无一失”。产品的可靠性是时间的函数，因而，有人将“可靠性”称为“质量的时间指标”。时间因素对于产品可靠性的影响是不可忽视的。

产品的可靠性指标与产品的技术性能指标之间还有一个很重要的区别，那就是产品的技术性能指标可以通过仪器的直接测量，用灵敏度、选择性、不失真功率、图像明亮度、清晰度、保真度来表示。而产品的可靠性指标是一个统计指标，只有在进行可靠性试验、统计分析及调查研究的基础上，才能对产品的可靠度、失效率、有效度以及寿命特征进行正确的统计评价。

可靠性指标的综合性决定了可靠性工作内容的广泛性；可靠性指标的时间性及统计性决定了可靠性评价和分析方法的特殊性。影响产品可靠性的因素是多方面的，既有原材料及元器件的因素，也有设备及系统工程方面的因素；既与设计生产技术有关，也与科学管理水平有关。可靠性工作具有科研和管理双重特性，可靠性管理和可靠性技术是可靠性工作中两个不可缺少的环节。

可靠性工作以实现用户或战术指标所要求的可靠性指标为目的。而质量管理则以实现产品的低不良品率为主要目标。可靠性管理中有“固有可靠性”与“使用可靠性”之分，而质量管理则强调产品生产过程中的质量控制。美国和日本的经验表明，20世纪70年代初期可靠性管理与质量管理逐步融合，最后形成质量保证体系。实际上，将设计阶段的可靠性活动、生产阶段的质量管理活动、使用阶段的维修保障与信息反馈活动互相结合起来，就是质量保证体系的主要成分。建立和健全质量保证体系是提高产品可靠性水平的一项十分重要的基础工作。因此，必须努力推行以可靠性为重点的质量管理活动，将全面质量管理活动推向新的阶段，努力提高产品的可靠性与质量水平。

1.4 可靠性工程的发展历程

1.4.1 概述

翻开可靠性工程的发展史，不难看出，可靠性的发展历程与产品故障密切相关，

由故障导致其发生，在与故障的斗争中不断发展和演进——是一个从对故障机理一无所知到探索出规律准确预测，从对故障的被动处理到主动预防的漫长发展过程。

可靠性工程技术同样遵循事物的发展规律，经历了从概念形成、建立、发展、成熟，并向纵深发展等阶段。

下面大致分 5 个阶段说明可靠性工程的发展历程。特别需要说明的是，以下所列的各阶段划分是依据世界范围内可靠性工程发展的主流情况而定的，美国等欧美发达国家发展快一些，而像我国等发展中国家发展得慢一些。举例来说，当欧美发达国家的可靠性工程在 20 世纪 60 年代进入全面发展阶段时，我国的可靠性工程仍然处于初步建立阶段。

1.4.2 概念形成阶段

这一阶段大致发生在 20 世纪 40 年代。在这一阶段，欧美等国开始注意到产品的故障，萌发并逐步形成可靠性方面的观念，英国和美国是可靠性思想的重要发源地。

可靠性的概念萌芽可追溯到 20 世纪 30 年代末 40 年代初。英国航空委员会协同有关部门在 1938 年开始对飞机的故障和飞机结构件的故障情况进行调查和统计分析，随后在其飞机适航性研究报告中首次用概率来描述飞机的可靠性和安全问题，这可看成可靠性观念的最早萌芽。

美国的可靠性工作是从电子管开始的。20 世纪 40 年代初，电台、雷达等各种复杂电子设备的发明和应用，大大提高了战场通信和侦测预警能力，但却故障连连，严重影响其正常效能的发挥。统计数据表明，该时段美国 60% 的机载电子设备运到远东后不能使用，50% 的电子设备在储存期间出现故障。经过分析，发现这些电子设备故障的主要原因是电子管的可靠性太差，因此，在 1943 年美国成立了真空管发展部，随后在国防部下设置了电子设备可靠性专门工作组、电子管顾问组、电子元件顾问组和导弹可靠性专门委员会。在电子工业协会下设置有电子设备质量鉴定过程研究协会。1949 年，美国“无线电工程师学会”成立了第一个可靠性与质量控制的专门组织——可靠性技术组。

原德意志联邦共和国（西德）在第二次世界大战期间，在研制 V1 火箭的过程中，最早提出了串联系统可靠性的概念——串联系统可靠性等于其各组成部分可靠性值之积。

苏联于 1946 年开始关注和研究可靠性问题。苏联的可靠性技术研究首先在宇航领域和武器研制方面展开，并逐步推广应用到一般民用设备。

1.4.3 建立阶段

这一阶段大致发生在 20 世纪 50 年代。欧美各国纷纷成立可靠性方面的组织机构，并创立可靠性方面的理论，开始探索实践。我国也开始从国外引进可靠性方面的理论和技术，建立相应的环境试验机构，开展电子产品环境试验方面的探索性实践。

20 世纪 50 年代初，通信装备频繁发生故障，武器系统的效能得不到很好发挥，加上高昂的维护费用，一直困扰着美国部队指挥部门和后勤保障部门的神经，也对美国国内武器研制厂商形成了巨大的压力。为此，美国军方和武器研制厂商开始了空前的可靠性研究，美国的学术界也参与进来，各部门（联合）纷纷成立与可靠性相关的组织机构，开展相应的研究和实践。

1950 年年底，美国成立了“电子设备可靠性专门委员会”。1952 年 8 月，美国国防部成立了一个由军方、工业部门及学术界组成的“电子设备可靠性咨询组”（AGREE），其任务是提出改善军用电子设备可靠性的措施，推动可靠性工程的发展。该组织于 1955 年制订了一项可靠性发展计划，包括从设计、研制、试验、生产、交货、储存及使用等各阶段的可靠性研究。AGREE 在 1957 年 6 月发表了研究报告《军用电子设备可靠性》。这个报告阐述了可靠性设计、试验等的方法和程序，确定了美国可靠性工程发展的方向，成为美国可靠性工程发展的奠基性文件。AGREE《军用电子设备可靠性》发表报告以来，美国各研究和标准化机构制定了许多有关可靠性与环境试验方面的标准。

美国国防部于 1958 年成立了“导弹可靠性特设委员会”（ACGMR），专门研究可靠性管理问题，为美国空军武器系统司令部起草设计、研制及生产可靠性管理大纲。1959 年 1 月，美国空军导弹系统分部出版了 AFMM-58-10《弹道导弹及航天系统的可靠性大纲》，这个文件后来成为空军采购用的主要可靠性管理规范。1959 年 3 月，空军颁布了 MIL-R-25717C《电子设备可靠性保证大纲》，规定了试产及批产电子设备可靠性保证的一般要求。

苏联在 20 世纪 50 年代后期已认识到发展现代化设备不仅需要质量控制及质量检验，还需要可靠性工程，并开始可靠性研究及寿命试验工作。1958 年，日本科学技术联盟成立了“可靠性研究委员会”，介绍可靠性文献及在企业界开展可靠性普及活动，并从美国引进了可靠性技术。但是，苏联、日本等国的可靠性工程是在 20 世纪 60 年代以后才得以快速发展的。

20 世纪 50 年代，我国在广州筹建了亚热带环境适应性试验基地，1955 年 12 月成立中国亚热带电信器材研究所（工业和信息化部电子第五研究所的前身，1956 年

更名为中国亚热带电信器材试验站、中国亚热带电讯器材研究所), 专门从事电子产品环境试验和亚热带防护措施研究。随后又在海南岛、上海、舟山、西北等地区设立了试验站, 并开始了人工模拟试验工作。从电子产品对环境的适应性试验逐步引入电子产品可靠性概念, 并展开初步的探索实践。

1.4.4 全面发展阶段

这一阶段大致发生在 20 世纪 60 年代。在这一阶段, 可靠性理论和工程技术得到快速、全面发展, 欧美等发达国家从标准化、设计分析和试验评价等方面展开卓有成效的研究和实践, 取得重要进展。我国也开始建立相应的可靠性机构, 开拓性地展开可靠性方面的研究和实践。

20 世纪 60 年代, 美国武器研制系统开始全面制定和贯彻落实可靠性大纲要求。在这 10 年中, 美国军事工业, 特别是航空及航天工业发展迅速, 先后研制、发展了“阿波罗”、“水星”等各种航天器, F-111、DC-9、F-15 飞机, M1 坦克、“民兵”导弹等。这些系统的研制, 对于电子系统的高可靠性要求, 为可靠性工程的发展提出现实的需求, 起到了很好的促进和推动作用。在这期间, AGREE 提出的并逐步完善的可靠性设计及试验方法被美国国家航空航天局 (NASA) 及国防部 (DoD) 接受, 在上述系统中, 特别是在电子系统研制中得到广泛应用。

这一时期, 美国已充分认识到可靠性管理的重要性, 军方已从可靠性工程的角度着手制定统一的可靠性大纲和要求, 并有计划地在武器系统的研制开发中强制实施。美国空军于 1961 年颁布 MIL-R-27542《系统、分系统及设备的可靠性大纲》, 1965 年美国国防部颁布了 MIL-STD-785《系统与设备的可靠性大纲要求》, 1969 年颁布了其修订版本 MIL-STD-785A, 进一步明确了武器系统和设备寿命周期中各阶段的可靠性要求和实施要点。

同时, 美国空军“罗姆航空发展中心”(RADC) 在 1963 年组建了“可靠性分析中心”(RAC), 以加强武器系统和设备可靠性方面的专业研究, 包括可靠性预测、可靠性试验、可靠性分析、数据应用等。

在这一时期, 美国军方在可靠性试验、预测和分析方面也得到全方位的发展。在技术标准方面, 1963 年美国国防部颁布了可靠性试验标准 MIL-STD-781《可靠性试验(指数分布)》, 并在 1965 年和 1967 年颁布了其修订版 MIL-STD-781A 和 MIL-STD-781B, 规定了可靠性试验的程序和方法。20 世纪 60 年代初期, RADC 的可靠性分析中心提出了加速寿命试验和筛选试验方法。在可靠性预测方面, 美国国防部基于收集的大量现场和试验的失效率数据, 1962 年出版了可靠性军用手册 MIL-HDBK-217《电子设备可靠性预计》, 1965 年发布其第一个修订版 MIL-HDBK-

217A。该手册提供了大量的电子元器件可靠性数据及分析方法,作为电子设备及系统可靠性预计的基础,在世界各国得到广泛应用,也被我国所采用。RADC 在 20 世纪 60 年代初率先开展故障物理研究,研究各种电子元器件的故障机理及故障模式,建立其故障物理模型。1962 年召开了“美国第一届电子设备故障物理年会”。NASA 在 20 世纪 60 年代初率先在航天器中开展了故障模式、影响分析(FMEA),“贝尔电话实验室”于 1961 年提出了故障树分析(FTA)方法,利用演绎方法分析“民兵”导弹的可靠性和安全性,取得良好效果。随后 FMEA 和 FTA 技术在其他工业领域得到广泛应用。到现在,这两个方法仍然是主要的可靠性分析方法。

可靠性工程的发展,很长一段时间是建立在对故障的统计分析基础上的,尤其是在发展的早期。在 20 世纪 60 年代,随着计算机技术的发展和运用,美国逐步建立起各种可靠性数据系统,如美国陆海空三军的弹道导弹数据交换网(IDEP)及失效效率数据交换网(FARADA)等。

20 世纪 60 年代初,苏联开始意识到产品可靠性的重要性,制定一系列措施来推动可靠性工程技术的发展。随后,开始注重可靠性理论研究和实用的可靠性工程方法,在 K-S 统计检验法及马尔可夫过程等方面取得成就,并在可靠性设计的余度技术、降额技术、系统综合等方面取得实践成果。

日本引进美国的可靠性工程经验和技能后,开始注意把可靠性、经济性和全面质量控制(TQC)紧密结合在一起,并在 20 世纪 60 年代中期建立了覆盖可靠性及质量领域的质量保证体系,把质量保证与可靠性作为 TQC 的重要内容。

英国在 1961 年成立了“可靠性与质量全国委员会”,1966 年成立了“质量与可靠性协会”,并开展了全国性的可靠性与质量年活动。20 世纪 60 年代中期,在英国标准局成立电子设备可靠性委员会,从 1966 年开始出版可靠性系列标准。

法国的可靠性研究工作始于 1962 年。在法国的全国电讯科学研究中心(CNET)下设有可靠性试验机构和数据机构,负责可靠性数据收集处理和研究可靠性试验方法。从 20 世纪 60 年代中期起,在法国军用电子设备合同中开始提出了可靠性要求,CNET 的相关可靠性机构制定各种可靠性标准和规范,以统一规范军用设备可靠性要求,以及可靠性预计、试验和分析的程序和方法。

作为我国建立最早的可靠性专业研究机构,工业和信息化部电子第五研究所(以下简称“电子五所”)在我国可靠性研究和实践方面担当了开拓者的角色。1960 年 12 月,第三机械工业部第十六研究所(电子五所前身)成立,开始将可靠性理论和技术引入我国,并在电子行业率先开展全国性的宣传和推广应用。在 20 世纪 60 年代,我国在雷达、通信机、电子计算机等方面由于频频出现的故障引发,提出了可靠性问题,并开展了元器件的寿命试验工作,分别对通信机、雷达、电子计算机等整机进行了初步探索,举办了一系列可靠性知识培训班。由电子五所等单位牵头开展研究和实践,其他一些厂所也开始建立可靠性试验小组,着手采取有效的可

可靠性设计措施。

1.4.5 趋于成熟阶段

这一阶段大致是从 20 世纪 70 年代初到 80 年代末。可靠性工程经过了 20 世纪 60 年代的全面快速发展后,在这一阶段,可靠性工程技术已日臻成熟,主要表现在成立全国性的可靠性管理机构和数据交换网;可靠性管理和技术手段日益丰富完善,可靠性标准体系基本确立等方面。

首先是全国性的可靠性管理和技术机构的形成。美国国防部于 1975 年成立了直属美国三军联合后勤司令部的“电子系统可靠性联合技术协调组”;1978 年该协调组改名为“可靠性、可用性及维修性联合技术协调组”,其管理职能扩大到非电子设备,负责制定美国国防部范围内有关可靠性、维修性的政策及指导性文件;组织并协调国防部军用标准、手册的制定和修改,以及重大的可靠性与维修性研究课题的实施。

为加强政府机构与工业部门之间的数据交换,美国于 1970 年 9 月正式成立全国性的数据交换网——政府机构与工业部门数据交换网 (GIDEP),并设立常设机构,制订交换网的章程。随后, GIDEP 兼并了 FARADA。1974 年欧洲电子元器件性能验证试验数据交换网 (EXACT) 与 GIDEP 建立电子元器件试验数据交换关系。到 1980 年,已有 220 个政府机构及 404 个工业部门加入了该网。到目前为止, GIDEP 仍然是国际公认的具有权威性的数据交换网,其主要职能是收集、储存、检索和分配有关材料、元件、部件、设备、系统的可靠性试验和使用数据,以及试验设备数据、标准试验方法与有关计量数据。

在这一阶段中,可靠性分析设计、试验和工具等方面都取得重要进展。这一阶段的发展特点包括以下几方面。

1. 可靠性设计方面

随着技术的进步,采用成熟技术、简化设计、降额设计等可靠性设计准则被总结出来,并得到更加严格的要求和强化实施。技术的进步,电路和器件的集成化,使得简化设计成为可能。NASA 在航天元器件的降额设计方面率先取得实践经验和成效,在 1983 年颁布了第一个降额设计方面的标准 MIL-STD-975《标准元器件降额准则》(Standard Parts Derating Guidelines)。

美国在 1984 年颁布的 MIL-HDBK-338《可靠性设计》是美国军用可靠性设计方面的权威手册,指导美军装备研制、采购、使用、维护。该手册总结了美国几十年来可靠性工程的发展经验,反映了美国 20 世纪可靠性设计水平,内容丰富、实用

性强。1988 年 10 月颁布 MIL-HDBK-338A (最新版本为 1998 年 10 月颁布的 MIL-HDBK-338B), 该手册全面地论述了系统、设备和元器件的可靠性分析、设计和管理的理论及方法, 并给出大量计算和实用实例。

2. 计算机辅助设计工具方面

在这一阶段, 计算机技术飞速发展, 计算机辅助设计及制造技术的应用可大大提高生产率、降低设计费用。目前这种技术已广泛用于可靠性、维修性及保障性分析中。第一个可靠性软件工具是“罗姆航空发展中心”设计开发的, 主要包括电子产品可靠性预计功能, 目的是减少复杂电子系统可靠性预计的时间、费用及人为误差。美国国防部于 1984 年 9 月成立了可靠性及维修性计算机辅助设计 (RAMCAD) 小组来协调三军的 RAMCAD 的研究工作, 并在随后开发出系统可靠性、维修性及可用性综合分析程序, 把元器件清单汇编、可靠性预计、FMECA、电应力及热分析、可用性分析及权衡研究等程序结合在一起, 可根据用户的要求自动计算系统的可靠性、维修性及可用性的参数。

3. 可靠性试验方面

这一时期主要是综合环境应力试验、环境应力筛选和可靠性增长试验等技术得到很好应用, 并颁布了相应的标准。

大量的使用经验及分析表明, 航空电子设备外场使用的平均故障间隔时间 (MTBF) 与在实验室中按照 MIL-STD-781B 试验得到的 MTBF 相差悬殊, 其主要原因之一是 MIL-STD-781B 不要求进行综合环境试验。1977 年颁布的可靠性试验标准 MIL-STD-781C 规定可靠性试验要在更符合实际工作温度、振动与湿度综合环境应力的条件下进行。

20 世纪 70 年代后期, 环境应力筛选试验得到重视。1979 年, 美国环境科学学会召开了第一届电子设备环境应力筛选试验讨论会, 研究应力筛选试验要求和军民用品的筛选标准, 发展元件、组件及设备筛选试验技术。同年, 美国海军颁布 NAVMATP-9492《海军制造筛选大纲》来指导这种试验的实施。

开展可靠性增长试验, 通过试验发现及分析故障、采取改正措施并验证改正措施的有效性, 从而提高产品可靠性的过程。美国自 20 世纪 70 年代后期开始研制的飞机强调通过可靠性增长试验来提高机载设备的可靠性。1978 年美国国防部颁布 MIL-STD-1635《可靠性增长试验》军用标准来指导这种试验的实施。

4. 对可靠性的认识不断深入, 颁布一系列与可靠性相关的法令和标准

在这一时期, 美国军方的可靠性观念发生了重大改变。在 20 世纪 70 年代初,

美国军方可靠性的首要目标是降低寿命周期费用；到了 20 世纪 80 年代，已从提高部队作战能力的角度出发来发展可靠性。装备的可靠性影响作战效能的情况不断发生，使得美国军方充分认识到以性能为导向的装备发展模式存在严重缺陷，必须把可靠性及维修性要求与性能要求同等看待，即可靠性、维修性与性能并重。为此，美国国防部于 1980 年 7 月颁布命令 DODD5000.40《可靠性及维修性》，规定国防部发展各种武器系统的可靠性和维修性政策，国防部各部门对武器系统可靠性和维修性的职责，以及武器系统采购中可靠性和维修性活动应达到的目标等。1982 年 2 月美国国防部颁布指令 DOD3235.1《系统可靠性、可用性和维修性试验与评价》，对系统可靠性、可用性和维修性实验与评价提出明确要求。为贯彻落实这些指令，至 20 世纪 80 年代，美国国防部新增、修订 40 多项有关可靠性及维修性的指令、标准及规范。美国空军也于 1984 年着手制订 2000 年的可靠性及维修性行动计划，并于 1985 年 2 月由空军部长及空军参谋长签署公布实施。该行动计划从管理入手，提出通过提高可靠性及维修性来提高部队战斗力、增强生存力、减少部署运输量、节省人力和降低费用的 5 项目标，并制定了一系列的实施办法。

5. 机械产品和软件可靠性技术

机械产品、计算机软件的故障和维修保障问题，在这一时期得到重视。在机械产品可靠性方面，其可靠性预计、设计及试验方法得到建立和改进，研究提出了大量的机械零部件的可靠性预计模型、分析方法和验证试验方案，并出版相应的报告。美国可靠性分析中心（RAC）着手编制和出版非电产品数据手册（NPRD）。

计算机的出现无疑极大地推动了装备的进步，但由软件故障引发的装备故障占比不断上升，使美国军方认识到，软件的可靠性问题将严重影响装备效能的发挥。软件可靠性问题逐步得到重视。军方通过不断完善软件的可靠性模型、建立硬软件的组合模型，并通过软件可靠性数据的积累，提高软件可靠性预测能力。同时，通过软件工程方法和质量控制，保证软件的开发质量。

6. 与可靠性相关的维修性、测试性、保障性等学科发展

1983 年 1 月美国国防部颁布 MIL-STD-470A《系统及设备维修性管理大纲》，强调将测试性作为维修性大纲的一个组成部分。1985 年 1 月美国国防部颁布了 MIL-STD-2165《电子系统及设备的测试性大纲》，把测试性列为与可靠性、维修性同等重要的特性，作为电子设备或系统的重要设计参数，并在研制过程中进行分析、验证、试验和评价。

这一时期，保障性得到美国军方的高度重视。例如，军用飞机的保障性直接影响出动架次率、后勤保障费用、保障资源要求和飞机部署等，因此，美国军用飞机

把保障性作为与飞机性能一样重要的设计参数。

7. 我国可靠性工程的发展

电子五所(1972年更名为中国电子产品可靠性与环境试验研究所,即如今的工业和信息化部电子第五研究所),对我国可靠性工程起到积极的促进作用。20世纪70年代,随着高可靠性工程的迅速发展,人造卫星、导弹核武器、地下及海底线缆工程都对元器件提出了高可靠性、长寿命的迫切要求,并要求各类电子元器件能经受多种复杂环境的严酷考验。从1973年开始,原国防科委及四机部数次召开可靠性工作会议,提出重点研究解决国家重点工程用元器件的可靠性问题,制订了地缆工程的可靠性计划,对元器件提出了可靠性指标。1974年12月专门讨论了提高尖端产品使用的半导体器件的可靠性问题。1976年召开会议,对尖端产品所需元器件做出了高可靠性要求的规划定点工作。1978年12月,在认真总结几年来开展电子元器件可靠性工作经验的基础上,提出并实施《电子产品可靠性“七专”质量控制与反馈科学实验》计划,要求选择富有经验的专业人员,采用高精度的专业设备,选取专用的原材料,按照规定的技术协议进行专批生产,并对产品按规定标准进行专门检验和专门筛选,建立专用的工艺流程记录卡,即“专人、专机、专料、专批、专检、专筛、专卡”的“七专”措施。这一措施对推动可靠性工作起到重要作用,经过10多年的努力,使军用元器件可靠性提高2~3个数量级。与此同时,在“两弹一星”研制过程中,周恩来总理提出“严肃认真,周到细致,稳妥可靠,万无一失”的16字方针,在整机系统可靠性设计上采取措施,保证了运载火箭、通信卫星的连续发射成功,以及海底通信电缆的长期正常运行。

在这一时期,北京市、天津市、中南地区、东北地区、西北等地区都举办了各种类型的可靠性培训班。1979年中国电子学会成立了“可靠性与质量管理学会”。1980年,我国组织建立了“中国电子产品质量与可靠性信息交换网”,并在电子五所设立了可靠性数据中心。该中心逐渐成为我国电子元器件可靠性信息中心。1981年4月成立了“中国电子元器件质量认证委员会”。1982年国家标准总局召开并成立了“全国电工电子可靠性与维修性标准化技术委员会”。1982年4月中国科学院数学学会运筹学分会召开了第一届可靠性数学学术会议。1983年宇航学会召开了可靠性学术讨论会。可靠性工作在各行各业迅速展开。

随着可靠性工作的迅速推进,群众性的可靠性试验研究工作正在全国各地不断地向前发展。这一时期,全国有20多个省市试验站,许多厂、所都成立了可靠性小组,开展了寿命试验与筛选试验工作,加强了产品的检验与可靠性设计工作,研制了可靠性与环境试验设备,建立了60多条“七专”质量控制实验线。随着可靠性工作的逐步深入,可靠性工作也从军品深入到民品中。定期进行质量评

比,对电视机实施可靠性指标考核等,使电子产品的质量管理与可靠性工作有了较大的进展。随着可靠性工作的进一步开展,可靠性活动的国际交流也增多了。美国、法国、日本等国的质量认证及可靠性研究机构先后来我国进行交流。我国也派代表出席了国际电工委员会(IEC)的各种专业会议,美国、IEC 等组织还邀请我国可靠性学者到美国进行访问考察。1985 年我国可靠性与质量管理学会举办第三次年会,美国、法国、日本等国家的可靠性专家纷纷来华参加可靠性学术交流活动。

在可靠性标准方面,我国制定了 GB 3187-82《可靠性基本名词术语定义》、GB 1772-79《电子元器件失效率试验方法》、GB 2689-81《恒定应力寿命试验和加速寿命试验方法》等可靠性标准。在军事领域,对部分型号和较大的系统提出定量可靠性要求,并为此而开展设计过程中的可靠性分配、预计、评估及分析工作,从而保证产品可靠性的不断提高,尤其是 1987 年颁布的 GJB 299《电子设备可靠性预计手册》和 1990 年颁布的 GJB 899《可靠性鉴定和验收试验》两项技术标准,对我国装备的可靠性预测和试验评价工作起到重要的推动作用。

从 1978 年开始,原国家计委、电子工业部及广播电视工业总局陆续召开了有关提高电视机质量工作会议,对电视机等产品明确提出了可靠性、安全性要求和可靠性指标,组织全国整机及元器件生产厂开展了大规模的以可靠性为重心的全面质量管理。在 5 年时间内,使电视机平均故障间隔时间(MTBF)提高一个数量级,使 MTBF 由 300 小时提高到 3000 小时,配套元器件使用可靠性也提高了 1~2 个数量级。

由于狠抓国家重点工程和电视机的可靠性,进而推动了整机和电子元器件可靠性工作。20 世纪 70 年代末到 80 年代初形成了我国可靠性工作的第一个高潮,全国各工业部门及各兵种纷纷进行可靠性普及培训教育,形成骨干队伍,建立可靠性工作组织管理机构,进行可靠性试验和可靠性设计,以及信息收集与反馈工作。

20 世纪 80 年代末,各级领导转变观念,重视产品质量,首先在装备上加强质量与可靠性工作,着力贯彻《军工产品质量管理条例》。《军工产品质量管理条例》明确提出对可靠性工作的要求,在研制阶段主要贯彻可靠性保证大纲,在生产阶段主要贯彻质量保证大纲。1988 年,我国制定了第一个装备可靠性纲领性文件——GJB 450《装备研制与生产的可靠性通用大纲》,对装备在论证、方案、设计分析、试验评价和使用阶段的可靠性工作全面提出了明确要求。通过宣传、贯彻 GJB 450《装备研制与生产的可靠性通用大纲》及 GJB 368《装备维修性通用规范》,1993 年原国防科工委颁布《装备可靠性与维修性管理规定》,于 20 世纪 80 年代末至 90 年代初掀起我国可靠性工作的第二个高潮,这次高潮的特点是:

- 树立当代质量观,把可靠性工作视为质量工作的组成部分。
- 自上而下狠抓可靠性工作。
- 转变观念,把可靠性指标与性能指标同等看待。
- 用户对产品可靠性十分重视,提出强烈要求。
- 开展系统的可靠性管理工作,对产品全寿命周期实施可靠性监控,制订出一系列的可靠性国家标准和国家军用标准。
- 加强了可靠性新理论、新技术的研究与应用,如计算辅助设计(CAD)、健壮设计、并行工程、田口方法等。
- 把可靠性工程技术引入到国家重点工程及装备的研制、生产与使用中,去,原国防科工委成立了可靠性工程办公室及专家组,在重点型号装备中开展可靠性工作。
- 重视、加强可靠性培训教育。在原国防科工委颁布的《关于加强军工产品质量工作的若干规定》的第二章“加强培训教育,提高队伍素质”中,提出五条具体详细要求。原国防科工委成立了可靠性教育培训中心,原电子工业部也成立了培训中心,编写、出版教材,进行培训考核,要求参与装备研制的人员持证上岗。

1.4.6 深入发展阶段

从 20 世纪 90 年代开始,可靠性工程向更深、更广的方向发展。

1. 国外可靠性工程的深入发展

可靠性工程的发展也经历了一个曲折过程,甚至一度出现了滑坡现象。在海湾战争后,美军推行采办改革,废止了部分可靠性标准,弱化了可靠性工作。在其后续新装备的研发过程中,可靠性相关问题不断。据 2009 年美国政府问责办公室发布的有关武器项目评估报告分析,在相关作战鉴定试验中,仅有 47% 的装备达到了规定的可靠性要求,而号称全球最先进的战机之一的 F-35,自装备至部队以来也事故频发。

近年来,美国经过深刻反思,重新强调可靠性等通用质量特性的重要性,并采取了一系列举措。包括以下几项。

(1) 颁布《采办改革法》

2009 年,颁布了《采办改革法》(Weapon System Acquisition Reform),明确要求在需求生成系统中,提出可靠性要求,后续纳入采办合同。美国国防部系统工程局希望通过系统工程,提高重大采办项目的可靠性水平。重大项目的采办要制订可

靠性等工作计划，并纳入项目系统工程计划。

（2）将可靠性作为装备性能的关键要素

在 2008 版美国国防部指示 DODI 5000.2《国防采办系统运行》、美国国防部技术备忘录 DTM 11-003《可靠性分析、规划、跟踪与报告》等文件中，将可靠性作为装备性能的关键要素，规定全系统、全寿命可靠性管理要求，强调要提高可靠性水平，保证装备作战适用性、降低采办成本。

（3）大力加强工程管理

拓展强化了美国国防部系统工程局的职能范围和作用，加强可靠性管理工作，相继恢复部分可靠性军用标准，与工业界合作制定了一些专项标准，编制大量手册和指南，有力推进可靠性工作的落实。

（4）发展故障预测与健康管理等智能化可靠性技术

故障预测与健康管理（Prognostics and Health Management, PHM）技术的发展，经历了一个漫长的过程。PHM 是在传统的状态监控和故障诊断技术基础上发展起来的，并随着装备性能和复杂性的增加，以及信息技术的发展不断演进，从对故障和异常事件的被动反应，到主动预防，再到事先预测和综合规划管理，大致经历如下 3 个阶段。

① 由外部测试到机内测试（BIT）。

早期装备较简单，一般由相对独立的模拟单元组合而成，主要采用人工测试手段进行故障诊断，需要将外部测试设备（不是装备的一部分）与被测对象连接，以便获取被测对象的状态信息，并进行测试和故障诊断。

对于某些关键的系统或设备，如飞机的发动机、燃油系统等，飞行员需要实时了解其运行状态，以便在其工作异常或部分故障时及时采取应对措施。这就要求被测系统本身具有一定的自动检测能力，于是嵌入式的机内测试（BIT）系统被研制出来了。后来 BIT 又被用于维修人员查找故障。随后 BIT 得到迅速发展，能够自动检测和隔离故障的机内测试设备（BITE）被广泛使用。

② 测试性和综合诊断学科的形成。

对于较为复杂的系统，需要通过综合运用机内测试和外部测试能力才能实现准确的诊断，这就需要在系统研制阶段进行测试性设计。在 20 世纪 80 年代中期，美国国防部颁布了军用标准 MIL-STD-2165《电子系统和设备的测试性大纲》，把测试性作为与可靠性、维修性同等重要的产品设计要求，使得测试性成为一门与可靠性、维修性等并列的独立学科。

美国国防部于 1991 年 4 月颁布了军用标准《综合诊断》（MIL-STD-1814），把综合诊断作为提高新一代武器系统的诊断能力和战备完好性、降低使用与保障费用

的一种有效途径。自 20 世纪 90 年代以后,英、法、俄罗斯等国也效仿美国的做法,提倡在武器装备中通过采用类似综合诊断系统方案的综合维修系统来实现最大的故障检测和隔离能力,以提高武器装备的战备完好性,降低寿命周期费用。

在 1999 年,美国国防部办公厅(OSD)启动了“综合诊断开放系统方法演示验证”(OSAIDD)研究计划,探讨统一的、通用的综合诊断功能实现方法的可行性,以降低费用,增加互用性。

③ PHM 系统的形成。

PHM 系统是在需求牵引、技术推动下,借助联合攻击战斗机(JSF)项目的研制契机诞生的。

随着系统复杂性、信息化和综合化程度的大幅度提高,以往的事后维修和定期维修已经无法很好地满足现代战争和武器装备对装备保障的要求,在这种情况下,美军在 20 世纪 90 年代末引入民用领域的视情维修(CBM),作为一项战略性的装备保障策略,其目的是对装备状态进行实时监控,根据装备的实际状态确定最佳维修时机和策略,以提高装备的可用度和任务可靠性。在 20 世纪 90 年代中期启动的 JSF 项目提出了经济承受性、杀伤力、生存性和保障性 4 个目标,并提出了自主式保障方案。借此机遇,研制了较完善的 PHM 系统。

美国国防部威胁减少局(DTRA)在 2000 年将 PHM 技术列入《军用关键技术》报告中,最新的防务采办文件将嵌入式诊断和预测技术视为降低总费用和实现最佳战备完好性的基础,进一步明确确立了 PHM 技术在实现美军武器装备战备完好性和经济可承受性方面的重要地位。目前,PHM 已成为美国国防部采购武器系统的一项要求。

美国国防工业协会(NDIA)在 2006 年 4 月公布了 NDIA 电子产品预测技术工作组的最终报告草案。该报告针对电子产品 PHM 技术需求明确了在软件工具、预测技术、模型和设备 4 个领域的开发需求。

国外参与 PHM 相关技术研发的单位很多,例如美国国防部和各军兵种的有关机构;NASA;波音、洛克希德·马丁、格鲁门、ARINC、霍尼韦尔、罗克韦尔、雷神、通用电气、惠普、BAE 系统公司、史密斯航宇公司、古德里奇公司和泰瑞达公司等跨国公司;康涅狄格大学、田纳西大学、华盛顿大学、加州工学院、麻省理工学院、佐治亚理工学院、斯坦福大学、马里兰大学等著名院校;智能自动化公司、Impact 技术公司、质量技术系统公司(QSI)、Giordano 自动化公司等软件公司;荷兰 PHM 联盟(DPC)、Sandia 国家实验室(SNL)、美国国防工业协会(NDIA)系统工程委员会、美国联合大学综合诊断研究中心、美国测试与诊断联盟(TDC)等协会和联盟。其中,研发电子产品 PHM 技术的单位首推马里兰 CALCE 电子产品和系统中心,其水平处于国际领先地位。



2. 我国可靠性工程的深入发展

自 20 世纪 90 年代以来,我国持续跟进国外相关机构的可靠性工程经验,深入开展可靠性技术和管理工作。原国防科工委和总装备部按照结合国情、积极采用先进标准的原则,组织制定和完善了可靠性及维修性的基础标准,包括 GJB 150《军用设备环境试验方法》、GJB 368《装备维修性通用规范》、GJB 450《装备研制与生产的可靠性通用大纲》等,逐步形成比较完善的可靠性及维修性标准体系。

为保证可靠性及维修性研究、设计、试验、管理工作的开展,加强学术交流,先后成立了中国电子学会电子产品可靠性与质量管理专业委员会、中国航空学会维修工程专业委员会、可靠性专业委员会、全国军事技术装备可靠性标准化技术委员会,以及航空、兵器、舰船、航天分委员会等专业技术组织。

自 21 世纪以来,国内对于可靠性工作的投入持续升温。2010 年,国务院、中央军委联合颁布了《装备质量管理条例》,对装备全寿命周期的可靠性等工作提出了明确要求,并将该项工作纳入法制轨道。2014 年 8 月,总装备部颁布《装备通用质量特性管理规定》,确定了装备全寿命周期通用质量特性(含可靠性、维修性、保障性、测试性、安全性和环境适应性)工作的主要内容和要求,旨在合理确定装备通用质量特性要求,监督控制各阶段通用质量特性工作的实施,提高装备战备完好性、任务持续性和装备完好率,降低装备保障资源需求和寿命周期费用。

同时,国内的科研机构、型号研制单位也逐步推进可靠性工程技术在型号中的应用,包括开展装备定延寿试验技术、失效物理技术、机械可靠性技术、通用质量特性综合应用技术、软件可靠性技术、软硬件可靠性技术、微机械产品可靠性技术、可靠性评估技术、网络系统可靠性技术、装备体系可靠性技术、PHM 等研究和实践,从宏观的体系到微观的失效物理,全面开展可靠性技术研究和实践,取得显著成效。另外,我国在电子产品可靠性基础数据资源建设、电子元器件质量控制与国产化管理等方面,也取得了重大进展。

同时,我国积极参与可靠性领域国际标准的制定工作。例如,我国华为技术有限公司和工信部电子五所等联合起草、制订了网络系统可靠性方面的标准,包括 IEC 61907 Communication Network Dependability Engineering(通信网可信性工程,在 2009 年 12 月颁布实施)和 IEC 62673 Methodology for Communication Network Dependability Assessment and Assurance(通信网络可信性评估和保证方法,在 2013 年 6 月颁布实施),这是国际上首次制订通信网络可信性方面的顶层技术标准。

3. 可靠性工程软件的发展

在计算机可靠性辅助设计软件方面,自 20 世纪 90 年代以来得到飞速发展。

20 世纪 80 年代开发的软件主要面向单一的可靠性工作项目,如可靠性预计、FMEA 等。随着可靠性工程和软件技术的发展,人们开始关注可靠性工作项目的内在联系和软件工具之间的数据共享问题,并由简单的文件交换数据向综合共用数据环境模式发展。

目前,装备可靠性工程软件已经完成了由单一软件工具向集成系统或集成平台的转变。国外比较典型的系统有美国 RELEX 公司开发的 Relex Studio (后为 PTC 公司收购,融入 Windchill WQS)、瑞典 Syscon 公司研制的 Syscon ILS、美国 Raytheon 公司开发的 EAGLE (Enhanced Automated Graphical Logistics Environment)、英国 Pennant 公司开发的 OmegaPS、美国 ISS 公司开发的 SLICWave,以及以色列 BQR 公司开发的综合保障软件 (CARE、CAME、CAFDE)、美国西南研究院 (SwRI) 开发的 NESSUS 软件、美国 DSI 公司推出的 eXpress、英国 Isograph 公司研制的 ISOGRAPH、美国 DfR Solutions 公司开发的电子封装可靠性设计软件 Sherlock 等。

我国可靠性工程软件的工具研制始于 20 世纪 80 年代末。1992 年 6 月电子五所依据其起草制定的国家军用标准 GJB 299 《电子设备可靠性预计手册》,发布了国内第一个商用化的可靠性软件工具——“电子设备可靠性预计与分配软件 EERP0692”,1997 年 7 月发布其 Windows 版本的工具 EERP0797。2000 年,在总装备部和原国防科工委的大力支持下,开展“电子设备可靠性预计技术与软件工具”课题的研究开发工作,研发形成“可靠性工程软件 CARMES-2000”,成为我国首个拥有自主知识产权并在可靠性行业具有广泛影响和应用的产品。经过鉴定,该软件达到当时国际先进水平,在软件功能、元器件可靠性数据库、工程实用性方面优于同期国外进口软件。

随着装备对通用质量特性管理需求的日益增长,CARMES 功能从可靠性设计分析拓展到维修性、保障性、测试性、安全性和环境适应性设计分析,从单一的分析计算到辅助设计,从设计阶段的预计分析到全寿命周期的五性指标论证、方案优选、设计分析、试验评价和使用保障,一步步向集成化、自动化、全寿命、全特性综合发展与演进。CARMES 全面融合我国工程所需 RMS 技术,立足国际前沿,密切结合工程实际,历经 11 个版本的升级,吸取了广大用户装备 RMS 工程的经验和方法,在安全保密、工程实用化、标准先进性、数据库支持、性价比等方面优于国外同类软件。最新版本 CARMES 7.0 包括 26 个功能模块,覆盖了型号通用质量特性管理、预计分析、设计、试验评价等工作项目,从型号通用质量特性管理一体化协同设计和全寿命/全过程/全特性管理需求出发,构建企业级可靠性协同工作环境和平台,提供通用质量特性工程一体化的解决方案。突破原有版本五性工具集的定位,从通用质量特性管理系统工程的角度统一筹划,强化通用

质量特性项目、任务、流程、状态和数据的管理监控,功能更加强大实用,可有效辅助企业全方位实现型号通用质量特性管理工作的顶层管理、过程协同和数据共享。在通用质量特性管理系统性、集成化、规范化、自动化和易用性方面取得重要进展。

CARMES 在国内工程中获得了广泛应用并取得应用实效,已成功应用于神舟飞船总体及各分系统,在中国电子科技集团、中国航天科技集团、中国航天科工集团、中国船舶重工集团、中国兵器集团、中国工程物理研究院下属 500 多家装备研制生产单位以及通信、家电等企业的广泛应用说明中,CARMES 可很好地满足可靠性/维修性/保障性设计、分析、评估和管理的需要。

CARMES 提供丰富的可靠性基础数据库,精选了工程常用元器件,构成可靠性预计参数库,按型号规格直接对应到 GJB/Z 299C 预计标准的详细类别,进行可靠性预计时可自动获取分类信息,具有工程的实用价值。CARMES 提供了建立通用设备可靠性参数库功能,用户可以根据工程的实际需要,建立本单位常用的通用设备可靠性预计数据库,实现设备级可靠性预计数据的共享,极大提高可靠性预计效率。CARMES 中的超过 50 万种型号规格的国产和进口元器件可靠性预计参数库,包括丰富的可靠性预计参数和优选信息。另外,还包括发动机、齿轮、陀螺等机电产品可靠性统计数据及预计模型算法,是国内目前最具工程实用性的数据库。

国内的北京航空航天大学、装甲兵工程学院、国防科技大学、军械工程学院、空军装备研究院航空所等也开发了相应的软件工具或平台。

1.5 可靠性工程的发展趋势和面临的挑战

1.5.1 概述

可靠性技术经过 70 多年的发展,已逐步形成较为完整的技术体系,可靠性建模、可靠性预计、FMEA、FTA 等工程技术已在工程中得到普遍应用,对提升产品可靠性、降低寿命周期费用发挥了重要作用。

可靠性的发展需求与技术的发展、产品的演进是密不可分的。近年来,随着工业技术、信息技术、原材料等的不断发展和进步,以及产品向复杂化、集成化、体系化、智能化、微型化、机电一体化、绿色环保和信息物理融合等方向演进,可靠性工程技术也快速向前发展。本节将结合当前技术、产品发展的现状和趋势,介绍和探讨可靠性工程方面的动态和发展趋势。

1.5.2 复杂系统的可靠性

1. 复杂系统的特点及可靠性问题

复杂系统（System Complexity）科学是近年来人们关注的一个热点，特别是美国桑塔菲研究所的创始人乔治·考温（George Cowan）把这个问题提升到“21 世纪的科学”的高度以来，人们对复杂系统科学的研究兴趣更是与日俱增。

复杂系统是具有复杂性属性的系统，它拥有大量交互成分，其内部关系复杂、不确定，总体行为为非线性，既不能由全部局部变量、局部属性来重构总体属性，也不能通过系统局部特性形式地或抽象地描述整个系统的特性。复杂系统的研究，具有下列几个特点：

- 系统的模型通常用主体（agent）及其相互作用来描述，或者用演化的结构描述。
- 以系统的整体行为，如涌现（emergence）等作为主要研究目标和描述对象，以探讨系统的一般化动力学规律为目的，例如，幂律（power law）、遗传规则、自组织临界性（Self-Organized Criticality）等。
- 强调数学理论与计算机科学的结合。元胞自动机、人工生命、人工神经网络、遗传算法等都可看成它的虚拟实验手段。

总体来说，复杂系统主要由行为、结构及管理共 3 部分组成。它们之间存在相互影响、约束的关系。例如，行为影响管理过程的执行，反过来，管理则约束行为，如图 1-4 所示。

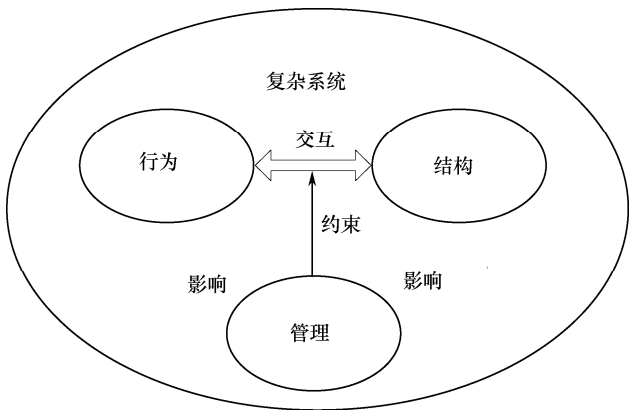


图 1-4 复杂系统结构图

复杂系统由于其行为特征与传统的简单系统相比有很大的不同，其可靠性建模、分析等方面也面临诸多挑战。

2. 复杂系统的可靠性建模

复杂系统的建模方法很多，其核心内容是要分层次建立集成模型，清晰地表征其功能、结构、流程和行为特性，以及它们之间的关联关系。以下给出复杂系统可靠性建模的基本思路。

基于复杂系统理论，以功能、流程模拟为核心，采用分层次、多因素、多维综合建模的方法，可建立复杂系统的一体化可靠性模型，综合表征可靠性目标与约束、系统功能、结构、流程及其交互作用和关系。

复杂系统的可靠性模型一般包括可靠性目标层、功能层、结构层、流程/控制/行为层、表示层/模型层共 5 个层次，如图 1-5 所示。

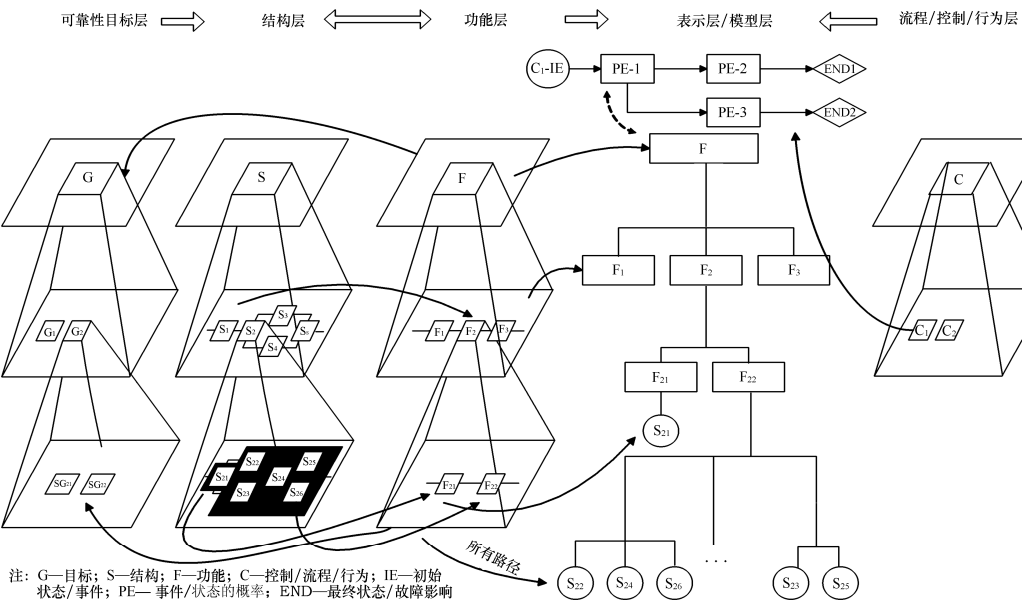


图 1-5 复杂系统可靠性建模示意图

这 5 个层次分别是：

- 第一层：可靠性目标层，描述系统的可靠性目标、要求和约束。
- 第二层：功能层，描述实现系统可靠性目标的具体功能。
- 第三层：结构层，描述实现具体功能的结构/设备。
- 第四层：表示层/模型层，可采用事件序列图/Petri 网等工具进行表示。
- 第五层：流程/控制/行为层，描述系统的任务、流程及事件演变过程。第五

层的任务、流程及事件，与功能层、结构层又是紧密关联的。

中外学者一直致力于复杂系统的可靠性建模与分析方面的探索实践，从不同角度给出复杂系统可靠性的解决思路。例如，应用 1982 年诺贝尔物理学奖获得者 K.G.Wilson 提出的重正化群变换理论（即相变的临界现象理论），一些学者通过研究复杂网络的渗流问题，给出了简化复杂网络系统结构、确定网络转变临界值的理论和方法；在斯洛文尼亚，由 Tadic 领导的研究小组利用信息熵理论，研究发现互联网具有长程时间相关性，其发生信息拥塞的原因，主要是因为信息包在某些中枢节点（Hub nodes）上等待的时间过长，为将网络的拓扑结构与具体的业务流相结合建模和综合分析提供了一种手段；我国工程院院士李德毅针对概率论和模糊数学在处理不确定性方面的不足，提出了云模型的概念，并研究了模糊性、随机性及两者之间的关联性，可应用于复杂系统分析中的定性概念到定量数值的转换。

3. 通信网络的可靠性问题

作为应用最为广泛的典型复杂系统，网络系统（如通信网络系统）的可靠性问题，近年来得到人们的普遍重视。通信网是一种使用交换设备和传输设备，将地理上分散的用户终端连接起来，实现不同终端之间信息交换的系统。通信网络系统是一种典型的复杂系统，拥有复杂系统的所有共同属性，主要表现在以下方面：

- 多样性。包括网络自身组成与环境的多样性、网络故障原因的多样性、网络故障模式的多样性、故障原因与故障模式对应关系的多样性等。
- 涌现性。各种通信终端、网络部件按照一定的连接方式组合成为一个通信系统，不同的通信时段，网络中的业务量可能有所差异，就可能产生终端或网络部件不具备或部分具备的特性，这就是网络本身的涌现特性。
- 网络故障的传播性。网络各组成元素之间相互紧密的耦合关系。例如，通信网络系统中某节点发生故障时，与之相关联的实际网络拓扑结构、路由发生变化；同时，路由、拓扑结构的变化反过来也影响故障发生概率、业务的变化，以及复合复杂系统所描述的行为与结构的交互特性。这种耦合关系会导致通信网络故障呈现较强的传播特征，包括同一层次之间的横向传播特性和不同网络层次之间的纵向传播特性。
- 时效性。信息通常仅在一定时间内对决策具有价值，响应时间在很大程度上制约着通信网络应用的效果。
- 非单调性。网络状态与组件状态呈现复杂的非单调相关性。
- 失效相关性。共因、级联失效对网络可靠性的影响更加突出。
- 时序性。网络状态不仅依赖于组件失效的组合方式，而且与其失效的先后

顺序密切相关。

- 非确定性逻辑。网络可靠性影响因素交错复杂，分析人员不可能面面俱到地分析网络及其组件之间的故障逻辑关系。
- 软件影响。软件对网络可靠性的影响越来越大，不容忽视。
- 人机交互。人在复杂工程网络中扮演着越来越重要的角色。
- 信息的不确定性。决策信息来源多样化，包括专家经验等，其中大部分都是不完整、不确定性信息。

复杂系统与通信网络系统的关系如图 1-6 所示。

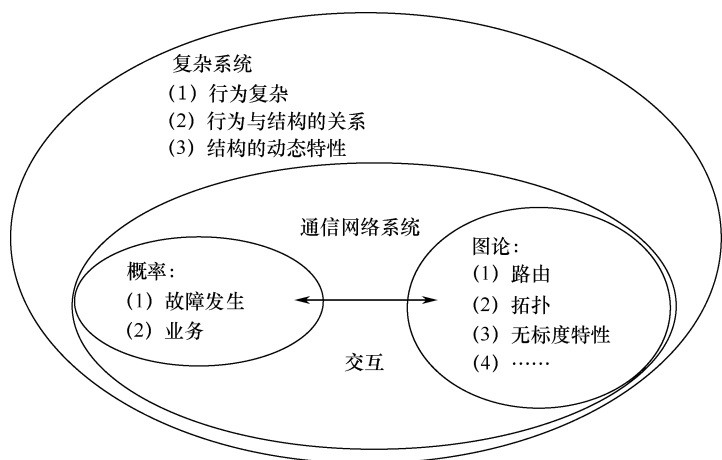


图 1-6 通信网络系统与复杂系统关系图

由图 1-6 可知，通信网络系统与复杂系统有密切的关系，如果抛开复杂系统理论来研究复杂网络系统的可靠性，往往是片面的。例如，一些学者将概率论和图论结合来描述通信网络的可靠性，从通信网络的拓扑结构及故障概率的角度提出网络的联通度、黏聚度、可靠度、可用度等可靠性相关参数，可在一定程度上反映通信网络的可靠性问题。然而，这样的描述无法反映通信网络拓扑结构与信息传递行为的关系，未能从通信业务的角度描述通信网络系统的可用性问题，因而是片面的，会与用户感知的网络业务可用度相去甚远。

因此，当前许多学者考虑从复杂网络系统本身的特性、发展规律出发，应用复杂系统理论研究复杂网络系统的内在本质与可靠性之间的潜在关系，以寻求有效解决复杂网络可靠性问题的方法。例如，通过离散事件仿真方法，建立网络拓扑结构和行为（通信业务、故障、修复）相结合的仿真模型，求解综合考虑网络结构与行为的业务可用性问题。

本书第 10 章将专门论述网络可靠性问题，这里不再赘述。

1.5.3 动态系统的可靠性

1. 动态系统的特点与可靠性问题

动态系统是指状态变量可能随时间发生演化的系统，这里的状态是指足以描述系统过去与现在演化特性的性状的最小集合。广义上的动态系统是个极宽广的范畴，也是前述复杂系统的一种。

现代系统主要表现出动态性、复杂性、顺序性、依赖性、非单调性、多态性和随机性等特征。动态性是复杂系统的一个重要特征，由于影响系统可靠性的因素多种多样，如系统硬件配置、软件和操作员行为、系统内部的动力学过程，以及系统与环境之间的相互作用、相互影响等，系统行为随时间的演化而变化，并且这种演化具有随机性。因此，在可靠性领域，动态系统指的是系统各组成成分（简称为“组件”）间相互作用、相互影响，系统的失效不仅与各失效组件的逻辑组合相关，还与各组件的失效顺序及系统先前状态相关的一类系统。动态系统的失效函数不能像静态系统那样简单地表示为各失效组件的逻辑组合。

例如，航天器中的电子系统就是一个典型的动态系统。航天器中的电子系统包括数据处理系统、测量系统、通信系统、辅助导航系统，以及制导、导航与控制系统，共 300 多个计算机模块，分布于航天器的各个部位，这些子系统既各司其职，又相互协作、相互影响，共同完成任务。航天器能否顺利完成任务，不仅取决于各失效子系统的逻辑组合，还取决于当时所处的状态、各子系统的失效时序等。

2. 动态系统可靠性分析面临的挑战

随着科学技术特别是计算机技术的发展，各种控制和容错技术广泛应用，现代系统越来越复杂，人一机一环境以及系统硬件和软件之间相互作用、相互影响，系统可靠性表现出动态性、非单调性、多态性、相关性和随机性等特征，由此也导致了一些特殊的可靠性问题，如故障安全性、维修有序性（如液位调节系统）、隐含相依性结构（如人机故障）、状态依赖性（即事件影响与其发生时的过程、系统状态及其持续时间有关）等，这些都为可靠性分析带来了许多困难。

动态系统对可靠性分析提出了更高的挑战，复杂性、顺序性、依赖性动态系统的 3 个典型特征，这些特征及其对可靠性分析的影响主要表现在以下方面。

（1）功能多，规模大

动态系统性能不断增强，功能日臻完善，在单一平台上综合多种自动化信息处理功能的系统已是屡见不鲜。比如，在航天系统发展的早期，航天器的功能单一，单独一台计算机系统足以完成空间目标任务，随着图像处理、海量数据传输、高速

通信、科学研究等需求的不断增长,越来越多的任务需要在航天器上完成,航天器上也需要加装越来越多的分系统,各分系统之间相互协作,共同完成任务。动态系统中所使用的子系统以及元器件数量不断增多,有些系统甚至包括了数以百计的子系统 and 成千上万的元器件。瑞典空间公司(SSC)于1999年研制的UoSat-12卫星中使用了约70个处理器;新加坡于2008年发射的用于多光谱照相的X-Sat卫星中,利用现场可编程门阵列(FPGA)集成了20个并行处理单元,每个处理单元包括StrongARM SA-1110处理器和64MB SDRAM存储空间,并行处理单元与星载计算机一起共同处理每个任务剖面(容量为15GB)的图形数据;而类似核电、空间站等大型系统中则包括为数众多的部件和设备。

这些动态系统的可靠性并非能用简单的模型加以分析。由于规模巨大,无论使用哪种可靠性分析模型,都有可能导致“组合爆炸”或“状态空间爆炸”问题,使得求解效率降低,有时甚至无法求解。

(2) 结构复杂,相互依赖

动态系统所处的动力学环境及其结构都极其复杂,另外,由于对高可靠性的需求,在系统设计阶段,融入了许多容错结构设计,客观上又增加了系统的复杂性。系统的复杂性带来了系统可靠性和安全性的下降,投资增加,研发周期加长,风险增加,并且由于产品复杂性的增加,必然使参与设计、制造、使用和维修保障全过程的单位和人员增加,人机交互复杂。

元件间的相互作用、相互依赖也越来越强。在传统的静态系统中,各元件之间可以认为是互相独立、互不影响,通过对各元件失效的布尔组合逻辑便可得到系统的失效函数。随着实践中对系统功能、性能和可靠性要求的提高,以及一些可靠性设计技术的应用,系统中各元件之间互相依赖,一个元件的失效可能使得其他元件无法正常工作,系统的失效函数也不能简单地通过对各元件失效的布尔组合逻辑得到。比如,为了提高系统的可靠性,目前的星载计算机中大多冗余了处理器、接口、总线、存储、电源等模块,而信息编码、看门狗、信号三模冗余(TMR)等容错技术的采用则增强了各个模块之间的关联。依赖性的增强,使得先前大部分可靠性分析研究中关于各元件相互独立的假设不再有效,从而增加了动态系统可靠性分析的难度。

(3) 失效参数复杂,失效模式多样

美国MIL-HDBK-217标准采用电子部件寿命服从指数分布的失效方式,然而,并非所有的部件寿命都服从指数分布,而且动态系统的工作环境并非完全支持指数分布的寿命特征。例如,在分析航天器的可靠性时,可靠性工程人员曾经建议部件的寿命采用Weibull与指数形式的混合分布,以便能够表示出典型的“浴盆”寿命曲线。当采用复杂的寿命分布分析动态系统时,某些传统的可靠性分析方法(如

Markov 链)和结论(如平均无故障时间是失效率的倒数)将不再成立。

系统的失效方式除了覆盖失效外,还有未覆盖失效。在有容错机制的动态系统中,由于故障不能被系统完整地检查、确定和恢复,从而使得系统的容错机制失效,元件的未覆盖失效(单点失效)行为会直接导致系统失效。

由于失效分布多样,大多数失效分布不能用规则的数学形式表达,利用数学分析建模方法一般很难单独确定出系统可靠性参数。不完全覆盖失效行为的建模及分析本身就极其复杂,动态特性进一步增加了系统可靠性的分析难度。

(4) 有顺序限制的失效模式

动态系统与静态系统的最大区别在于,前者失效模式可能不仅仅包括基本元件的静态逻辑组合,还可能依赖于其他元件是否失效(如储备系统)以及发生的时序等,也就是说,系统各元件的失效必须满足一定的顺序关系,才可能导致系统的失效。例如,假设系统中存在一个正常工作的处理器模块和一个冷储备的处理器模块,两个模块利用一个切换开关相连。如果切换开关在工作模块失效之后才失效(此时,原来的冷储备模块已经进入工作状态),那么系统仍将继续工作。但如果切换开关在工作模块失效之前发生失效,将会导致冷储备模块无法进入工作状态,使得系统在工作模块失效的时刻立即发生失效。在该例中,系统失效的判定标准不仅依赖于基本元件的组合,而且还依赖于基本元件失效的发生顺序。

由于动态系统的工作过程呈现出各种动态特性,如顺序失效、冷储备、功能相关等,已不能使用传统的基于割集的失效模式对动态系统进行定性和定量的可靠性分析,从而使得系统可靠性分析面临着越来越大的挑战。

3. 动态系统可靠性分析方法

针对工程实践和科学研究中不断出现的新情况和新问题,在现有国内外有关可靠性分析研究的基础上,根据动态系统的新特征,业界陆续提出各种新的可靠性模型,如美国弗吉尼亚大学的 Dugan 教授等人提出来的描述和分析动态系统的动态故障树; Tang 等人提出利用最小割集方法,分析动态系统的失效模式;利用不完全覆盖模型来分析不能充分检测错误、隔离错误或从错误中恢复的情况下容错的动态系统可靠性;使用 Markov 模型分析某些特殊的动态系统的可靠性并进行专门的优化;利用着眼于系统状态及其动态变化的随机 Petri 网 (SPN),通过赋予变迁以一定的延迟时间,对动态系统可靠性进行研究;利用贝叶斯网络模型对某些状态空间模型(如 Markov 链模型)难以处理的动态系统的可靠性进行分析;利用计算机仿真方法来对动态系统的可靠性进行研究,在某些情况下也是唯一可行的方法。

综上所述,在动态系统的可靠性分析方面已经取得了一定的成果,但显然远不能满足现实的可靠性分析需求。模块化分析、失效模式、不完全覆盖和可靠性仿真

是可靠性分析领域的重要研究内容，许多学者也进行了广泛的研究。由于动态系统存在复杂性、动态性和依赖性等特征，这些特征共同存在，互相影响，使得以上研究内容已不能或仅部分适用于动态系统，进一步开展动态系统可靠性技术研究具有迫切需求和重要现实意义。

1.5.4 体系的可靠性

随着体系研究的日益深入，体系的内涵也在不断充实和演进。一般而言，体系是为实现共同目标聚合在一起的大型系统集成或现网络。

尽管大量专家学者从不同角度对体系的定义和描述呈现多样性，但都体现了下列基本特征：

- 体系各成员系统的存在都是为了总体目标的实现。
- 各成员系统是彼此独立、分布的，具有不同的管理主体，为了持续地执行体系任务而集成在一起。
- 各成员系统间的联系是多种多样并且不断演化的。
- 体系各成员行为的累积及成员之间的交互导致不可预见的涌现行为。
- 体系的边界是模糊的或者是不断变化的，与环境的交互具有不确定性。

根据前述复杂系统的定义，不难看出，体系同样具有复杂系统的特征，也是复杂系统的一种。

下面以军事装备体系为例，研究其可靠性问题。装备体系是根据军事需求、经济性和技术可能，由一定数量和质量相互关联、功能互补的多种装备，按照装备的优化配置和提高整体作战能力的要求，综合集成的装备类别、结构和规模的有机整体。装备体系由战斗装备、保障装备组成，并随军事需求的变化和科学技术的发展而演变。

装备体系可靠性是其战斗力形成和保持的重要基础，直接影响装备系统的作战模式、作战规模以及持续作战能力，影响战斗力的巩固和提高，直接影响体系的作战效能。但由于装备体系规模大、层次多、组成复杂，各组成部分彼此是分离的，甚至是有地理或空间距离的，隶属于不同部门管理、使用，同时又是不断发展演化的，开展可靠性分析时，要考虑设备的硬件可靠性、软件可靠性和设备间的连接可靠性，还要考虑多时空、不同进程的可靠性等多种因素，传统的产品可靠性建模方法显然难以有效满足装备体系的可靠性建模要求。

现代战争越来越多地体现装备体系与体系之间的对抗，各类装备和作战单元之间的联系越来越紧密，日益成为一个有机整体。单个装备的可靠性高并不能代表体系的可靠性高。从体系出发，研究装备在体系中的配置关系，分析体系的可靠性是装备作战效能评估的重要内容之一。

目前,国内外关于装备体系的研究大多集中于体系的需求建模和结构优化方面,可靠性方面的研究才刚刚起步,国内外的相关文献较少。2008年,美国田纳西大学的 Mo Jamshidi 在论文《体系工程——21 世纪的挑战》中提出了体系可靠性是体系工程的重要目标之一。2009年,美国陆军装备研究发展中心(ARDEC)的 J.L.Cook 建立了体系的多状态系统可靠性模型,但是该模型仅对体系的基本可靠性进行粗略评价,对于体系的层次性、动态时序等特点考虑不足。

为此,国内外的相关机构对装备体系的可靠性进行了相应研究。目前,对于装备体系可靠性的研究,通过不同类型的模型(如任务建模、Petri 网、仿真等模型)或方法求解体系可靠性问题,归纳起来,大体有以下 3 类方法。

1. 基于流程的装备体系可靠性建模与仿真

由于装备体系的任务类型和任务阶段多,各系统之间的可靠性逻辑复杂,基于计算机的仿真无疑是进行可靠性分析的有效途径,因而,建立准确的可靠性仿真模型成为可靠性评价的重点。传统的可靠性模型,如可靠性框图模型、故障树模型、事件树模型与 Markov 模型,应用于装备体系任务可靠性建模分析与评价时难以描述装备体系的层次性、动态时序等特点,而 Petri 网作为离散事件仿真的通用建模工具,能很好地表示系统的同步、并发等复杂性质,能清楚地表示系统的动态行为,从而为可靠性分析提供了新的建模思路和方法。

目前, Petri 网已广泛应用于可修系统的可靠性建模与分析方面。例如,原菊梅总结了国内外基于 Petri 网的系统可靠性建模现状,针对传统 Petri 网模型的节点多,规模庞大的不足,提出了基于着色 Petri 网的复杂系统任务可靠性的建模方法。这种方法虽然在一定程度上减少了模型的规模,但是没有考虑装备体系的层次性问题,建模过程复杂、模型庞大。如果直接由人工据此建立装备体系任务可靠性 Petri 网模型,不仅工作繁杂,而且极易出错。对超大规模、异常复杂的装备体系的任务可靠性建模,必须考虑模型的自动生成技术,并用规范、直观的方式解决用户输入的效率和准确性问题。

针对传统可靠性模型在装备体系建模中存在的描述能力不足、Petri 网建模存在的模型爆炸和模型构建困难问题,一些学者将面向对象的思想与 Petri 网相结合,采用面向对象 Petri 网进行装备体系可靠性建模,取得较好效果。

2. 基于任务的装备体系可靠性评估

第二种方法是基于体系任务的可靠性评估。考虑到装备体系的功能是通过完成各类作战任务而体现的,对装备体系的任务可靠性进行评估更有其现实意义。作战任务是一定环境和时间条件下,为达成特定作战目标,由不同装备共同进行的一系列相互关联的作战活动的有序集合。对于装备体系而言,装备体系的作战任务是由

一系列围绕体系作战目标、由不同装备（系统节点）共同进行的作战活动组成的。基于任务的装备体系可靠性评估的主要步骤包括：

- 确定和定义作战任务的目标。作战任务的目标是指作战任务的完成条件或目标。
- 作战任务的装备（系统节点）。作战任务的装备是指参与完成作战活动的各类装备，即装备体系中的系统节点所构成的集合。
- 定义作战任务的活动。作战任务的活动是作战任务的基本元素，具有不可分割性和特定目标性。它是指在满足一定的条件下，可由一定的作战系统根据相关的规则、条例、条令完成过程动作。
- 作战任务的活动间关系。作战任务的活动间关系是指作战活动之间的相互约束和逻辑关系。由于作战活动的动态性，使得作战行动在实施时存在一定的逻辑关系。
- 作战任务建模。对于任何一个作战任务，都可被形式化地描述为上述 4 种元素的组合。
- 根据任务目标和作战任务模型，用解析、仿真等手段评估装备体系的任务可靠性。

国内研究人员借鉴了基于美国国防部体系结构框架 DoDAF（Department of Defense Architecture Framework）的装备体系需求开发技术思路，采用 UML 语言对装备体系的层次结构及任务进行可视化描述，建立装备体系的层次结构及任务描述模型，并以此作为基础，生成用于装备体系可靠性仿真的 Petri 网模型，在武器装备体系任务可靠性建模方面取得理论和实践成果。

3. 基于网络理论的装备体系可靠性建模

由于装备体系一般可以建立起网络模型，因此，一些研究人员考虑采用网络理论，将装备体系的可靠性模型以网络模型来表示，例如采用网络关联图的方式来描述，再应用网络可靠性理论解决体系可靠性的部分问题。

1.5.5 软硬件综合系统的可靠性

1. 软硬件综合系统的定义

基于微电子技术和嵌入式软件，实现信息共享、系统集成和智能化控制的系统（产品）称为软硬件综合系统。例如，飞机的综合航空电子系统和数字化飞行控制系统，航空发动机的智能化控制系统，通信网络的智能化程控器，电

网系统的智能化控制装置，汽车的自动挡传动系统，电脑控制的家电产品等。软硬件综合系统（产品）的发展和大量使用体现了技术进步以及社会生产力的发展，对于这类产品，尤其是大型、复杂软硬件综合系统的质量与可靠性管理具有重要作用。

2. 软硬件综合系统的质量与可靠性管理

软硬件综合系统的质量与可靠性管理的原则是在坚持硬件产品质量与可靠性管理的基础上，贯彻软件工程化要求，加强嵌入式实时控制软件开发的质量管理，实现软硬件综合系统质量与可靠性管理的一体化。

许多在硬件系统的质量与可靠性管理中行之有效的办法，如制定质量保证大纲；可靠性、维修性大纲；产品特性分类和关键件、重要件控制；分阶段的质量控制和设计评审；设计的验证与确认；贯彻可靠性、维修性、测试性设计准则；可靠性、维修性、测试性的分配和预计，元器件的质量与可靠性管理；FMECA 分析；FTA 分析；可靠性试验；综合保障分析与设计，以及故障报告、分析与纠正措施系统（FRACAS）的运行等均应全面贯彻执行。

（1）技术状态管理

技术状态管理包括技术状态标识和技术状态控制两个方面。

- 在技术状态标识方面，应当像对硬件的零部件一样，为每个具有独立载体（如 EPROM）的嵌入式软件标识一个图号，并根据系统分解结构，对功能进行划分，将软件纳入系统的配套表，实施技术状态管理。
- 在技术状态控制方面，所有子系统（设备）的技术规范必须经系统总设计师的批准；软件的需求规格说明必须经软件委托方和开发方会签同意；凡涉及总体技术指标（包括可靠性指标）、外形尺寸、软件需求、软硬件接口、环境和电磁兼容试验条件、质量保证要求等的更改，必须由提出方办理书面的要求（如技术协调单），经有关方协调后达成一致，并经设计师系统批准后生效、实施。在单位内部，需对已经冻结的技术状态和软件配置进行设计更改时，必须办理书面的更改手续，按技术责任制审签、会签和批准后生效、实施。

（2）供应商质量保证和系统工程管理

为了全过程地监控供方产品的研制质量，应当采用签订工作说明（SOW）作为技术经济合同的附件办法（详见 GJB 2742-1996《工作说明编写要求》），以便提高配套子系统（产品）研制工作的透明度，有利于合同委托方对供方研制工作进行全过程的质量监控。

对于大型复杂的软硬件综合系统，应当建立由所有参研单位参加的项目（型号）设计师系统和质量师系统，以便组成跨部门、跨单位的研制团队，在设计开发和质量保证两个方面密切协同，并实施系统工程管理。

（3）动态模拟综合设施的开发

动态模拟综合设施是能够全面模拟软硬件综合系统工作环境的计算机系统，应当在产品系统方案论证时同步论证并开发。该设施能够用于软硬件综合系统的人机界面开发，软件的测试与综合，软硬件的测试与综合，以及软硬件综合系统的验收等。

（4）系统的模拟综合

通过建立产品及其工作环境的数学模型，模拟产品的使用情况，对各子系统（配套产品）进行综合或集成，把大量问题暴露在设计阶段，并找出解决方法，解决可能出现的问题，大幅度地提高产品开发质量和效率，其中当前被广泛使用的一种方法是利用计算机，建立产品模型，设置对应参数，模拟该产品在实际工作中的环境，通过全数字仿真，对产品进行全面检查，以便找出潜在的问题。

（5）软件模拟器的开发

软件模拟器是模拟子系统（设备）接收输入信号、进行正确处理后输出信号的计算机软件（信号处理通过数学模型实现），其主要是在系统开发早期使用，具体用途主要分为两个阶段。

- 在各子系统（设备）的硬件研制未结束前，将软件模拟器在动态模拟综合设施上进行交联和运行，以验证各子系统（设备）软硬件接口关系的正确性，及时纠正软硬件接口设计的错误。
- 在各子系统（设备）的硬件和软件开发完成后，逐个利用真实子系统（设备）替代各自的软件模拟器，在动态模拟综合设施上进行综合和验收，直至所有的软件模拟器均被各自的真实子系统（设备）所替代。

（6）验收试验规范和验收试验程序的制定和贯彻

根据系统和子系统的技术规范分别制定各级产品的验收试验规范（ATS）和验收试验程序（ATP），自下而上地对设备、子系统、系统执行验收试验程序，进行全面、系统的测试和验收。

（7）动态模拟综合试验管理

动态模拟综合设施经严格的评审、鉴定后才能投入使用，分别针对人机界面的开发，软件的测试与综合，软硬件的测试与综合，以及软硬件综合系统的验收等任

务,制订动态模拟综合试验的计划,编制试验任务书、试验大纲,详细进行试验记录,运行 FRACAS 系统,对于试验中出现的故障采取纠正措施并进行归零管理。

3. 软硬件综合系统的可靠性分析与试验评价

软硬件结合系统的建模问题较为复杂,重点需要考虑软硬件之间的耦合和相互影响。

在试验评价方面,一般是通过构建软硬件结合试验剖面(即在系统使用剖面中注入软件运行剖面,两者叠加),对软硬件综合系统进行综合试验评价。我国一些机构已展开这方面的研究,并在机载雷达等系统中取得初步应用成效。

1.5.6 信息-物理融合系统的可靠性

1. 信息-物理融合系统的内涵

信息-物理融合系统(Cyber-Physical Systems, CPS)是多维异构的计算单元和物理对象在网络环境中高度集成交互的新型智能复杂系统,通过 3C(Computation、Communication、Control,计算机、通信和控制)技术的有机融合与深度协作,实现大型工程系统的实时感知、动态控制和信息服务,具有实时、鲁棒、自治、高效和高性能等特点。CPS 实现计算、通信与物理系统的一体化,可使系统更加可靠、高效、实时协同,具有重要而广泛的应用前景。

CPS 可以理解为基于嵌入式设备的高效能网络化智能信息系统,它通过一系列计算单元和物理对象在网络环境下的高度集成与交互来提高系统在信息处理、实时通信、远程精准控制及组件自主协调等方面的能力,是时空多维异构的混杂自治信息物理系统通过人机交互接口实现和物理进程的交互,使用网络化空间以远程的、可靠的、实时的、安全的、协作的方式操控一个物理实体系统。CPS 是构建在物联网之上,集计算、通信与控制于一体,实现物理系统与计算系统有机融合的系统,是装备智能化发展的方向。近年来,CPS 不仅已成为国内外学术界和科技界研究开发的重要方向,也是政府和企业界优先发展的产业领域,开展 CPS 研究与应用对于加快我国培育推进工业化与信息化融合具有重要意义。

目前,国内外相关机构的研究人员正在研究和发展基于模型定义的 CPS 建模技术,基于标准的 CPS 分层次集成技术,以及支持异构组件的 CPS 验证与测试技术等。

2. CPS 系统的可靠性问题与对策

以 CPS、3D 打印技术等为代表的工业方式变革,以及第四次工业革命下的信息技

术与制造业的深度融合等，对可靠性工程技术提出了新的要求和挑战。

可靠性是大型复杂系统的重要技术指标。广义的 CPS 可靠性涵盖了信息与物理组件的交互、软硬件结合组件可靠性、通信网络可靠性（含联通性、及时性、正确性、完整性）、信息安全和系统恢复性等方面。在 CPS 环境下，信息与物理组件间的交互与原有网络通信结构相比较更为频繁、方式更为丰富多样，网络中用户（或者智能组件）的地位也享有更多的平等、自由。此外，物理组件与面向对象的软件组件对于信息安全的标准也有本质不同，传统的单一基于线程和方法调用的模式将不再适用。在这样的环境下，如何提高 CPS 网络及相应组件的可靠性和抗毁性，保证用户的通信隐私，并实现在不确定复杂环境下对系统时间轴上不间断的监控与管理，是极富挑战性的关键问题。

（1）可靠性方面的挑战与对策

CPS 可靠性方面最大的挑战是：网络故障会阻碍 CPS 的实时运行。目前通用的网络技术（如 TCP/IP）是基于 Best-effort 思想建立的。这里，Best-effort（尽力服务）是一种服务模式，即当网络接口发生拥塞时，不顾及用户或应用，马上丢弃数据包，直到业务量有所减少，不再拥塞为止。Best-effort 对于高实时性要求的 CPS 应用，很难实现可预测性的保证。由于通信网络存在各种复杂因素，例如拥塞和信道质量造成了传输延迟、延迟抖动和丢包，会严重阻碍 CPS 数据包的实时传送。最终不可预测的传送时间必然会影响到被控物理系统的性能，甚至导致物理系统的不稳定。

相应的对策是：一方面可以通过增强系统的实时性来实现；另一方面，也可以借助现有的一些网络抗毁与级联事故预防技术，研究实施有效预防突发异常事件的处理机制，或者实现系统实时恢复的预警预报和在线修复技术。同时，保证系统能量的恒久维持也很重要，比如通过各组件之间的协调和调度来实现生产系统的不断电，或是研发使用寿命更长的新型储能设备等。

（2）信息安全方面的挑战与对策

CPS 的信息安全属于广义可靠性问题，这里仅做简单的讨论。CPS 的实时、自治等特性为其信息安全带来了许多新的问题，包括：

- 如何保证 CPS 在遭到恶意攻击时的实时性需求。
- 如何处理针对控制环节的恶意攻击。

CPS 为信息安全引入了物理因素，比如以物理进程为目标的攻击。更重要的是，如果攻击者成功地利用了 CPS 的控制能力，后果将非常严重。现有的计算机安全技术还没有足够的能力保证 CPS 的安全性。

CPS 在信息安全方面的主要对策有：

- 及时发现网络威胁，并预计攻击可能导致的结果。
- 认识到 CPS 在安全性防护中与传统信息系统的不同之处。
- 考虑建立从预防、检测、防御性修复、系统复原和制止相似攻击等几个层面来抵制攻击的 CPS 安全机制。其中，在预测阶段可以结合网络科学、社会科学和动力学等知识，例如偏好分析、行为发现、渗流预测等技术实现对可能存在威胁的感知，并及时发布预警。

1.5.7 云计算系统的可靠性

1. 云计算概述

云计算（Cloud Computing）是一种基于互联网的计算新方式，通过互联网上异构、自治的服务为个人和企业用户提供按需使用的计算。从用户视角来看，云计算是这样一种计算形式：与大规模信息技术相关的各种计算资源和计算能力通过互联网以服务的方式提供给用户。云计算通过互联网提供动态易扩展而且虚拟化的资源。终端用户不需要了解“云”中基础设施的细节，不必具有相应的专业知识，也无须直接进行控制，只关注自己真正需要什么样的资源以及如何通过网络来得到相应的服务。

全球云计算产业处于高速发展时期，市场规模不断增大，将会引导传统 ICT（信息通信技术）产业向社会化服务转型，未来发展空间十分广阔。2011 年全球云计算服务规模约为 900 亿美元，美国云服务市场规模约占全球的 60%，远高于欧洲（24.7%）、日本（10%）等国家和地区。云计算服务市场规模总量在 2011 年仅占全球 ICT 市场总量的 1/40，但增长迅猛，未来几年年均增长率预计将超过 20%，可见云计算的发展空间十分广阔。

各个企业或者研究机构所提出的云计算解决方案共同构成了一个生态系统，从各种已有的云计算技术形态来看，各家的云计算平台虽然各有不同，但是都满足以下技术特征。

（1）以服务的形式提供计算资源和计算能力

各种计算资源或计算能力通过网络以服务的形式提供给用户使用，这些资源具有不同的类型，处于不同的系统层次，从最底层的 CPU、磁盘、网络连接等硬件资源，到整个部署平台或运行环境，再到各种特定领域或业务的应用系统。

（2）支持多租户的网络访问和使用

不管所提供的资源处于哪个系统层次，用户都可以通过网络访问和使用，由于是面向多用户的，系统必须提供相应的机制为多个用户分配、维护和管理所需要的资源，这通常在虚拟化、分布式计算、分布式存储等技术的基础上实现。

（3）按需使用的弹性架构

根据需为用户分配资源，当用户的资源需求增加或者减少时，能以足够快的速度为用户重新分配或释放相应资源，从而提高资源利用率，减小用户的成本。这通常需要某种形式的负载均衡技术实现。

（4）最小化的管理负担

用户只需要很少的配置就可以使用各种计算资源和计算能力，而不需要参与对所使用资源的管理和维护，这要实现自动的动态资源配置和管理。

（5）按使用量支付

用户根据对资源的使用量支付相应费用，因而需要云计算系统可以对资源的使用情况进行实时的监控和度量。

2. 云计算可靠性面临的挑战

云计算发展迅猛，日新月异，大量的新技术涌现，因其拥有清晰的商业模式、高度可扩展的弹性交付服务方式、资源虚拟化、资源的自动管理与配置、海量数据的分布式并行处理、低成本并对用户透明和较高的可信性（即广义的可靠性）等特性，成为目前最受关注的技术热点之一。但是，云计算系统的可信性、数据安全等仍被大多数的企业和用户所质疑，在一定程度上妨碍了云计算的大规模应用。埃森哲研究院对影响云计算的因素统计分析数据颇具典型性，在所有影响云计算系统应用的因素中数据安全、可靠性分别排在第一位（89%）和第四位（75%），见图 1-7。

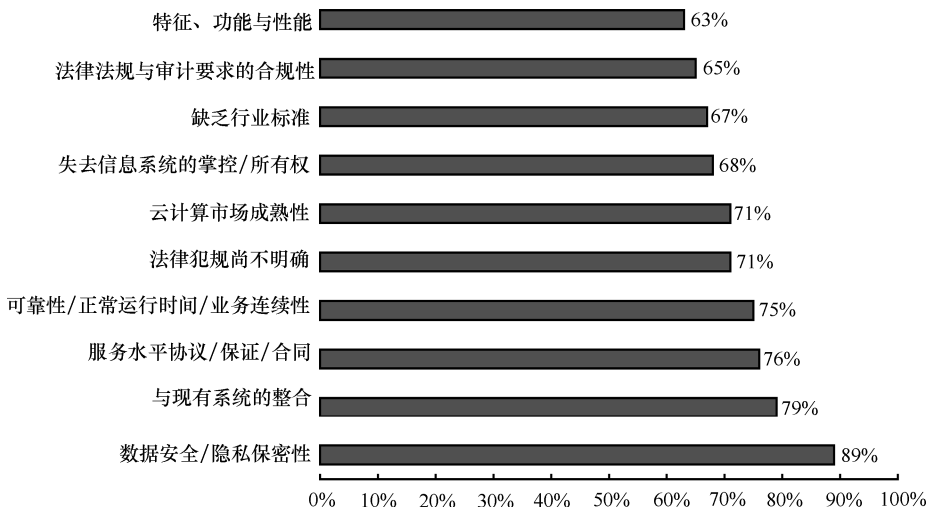


图 1-7 影响云计算应用的因素统计分析

云计算系统的可信性问题与其本身的特性密切相关，主要面临的挑战有以下几方面：

- 超大规模：出于成本的考虑，云计算中的单个计算机系统可能是由日用的、不可靠的部件组成。大规模的采用这些不可靠部件对整个云计算平台的可用性、可维护性以及容错性提出了严峻的挑战。
- 单一接口：云计算平台通常给用户提供的是一个统一的接口。大量用户通过这个统一的接口对云计算平台进行访问。
- 跨组织性：云计算平台通常通过租赁的方式提供给多个不同的个人与组织。这些个人与组织之间通常是互不可信的，甚至可能互为竞争对手。这就要求云计算平台能对各个用户之间的服务进行有效隔离，以保证数据的安全性与完整性。
- 以服务为中心：云计算平台是以服务为中心的，暂时的或者永久的系统维护与故障不能影响向用户提供持续服务。

3. 主要对策

（1）利用云计算的虚拟化特性提高系统可靠性

虚拟化是云计算的本质特征之一。著名的计算机科学家 David Wheeler 断言：“计算机科学中的任何问题都可以通过增加一个间接层来解决。”云计算的虚拟化技术正好可以提供这样一个间接的逻辑层。

虚拟化是指计算机元件在虚拟的基础上而不是真实的基础上运行。“客户”操作系统通过虚拟机监视器（Virtual Machine Monitor, VMM）来与硬件进行通信，由 VMM 来决定其对系统上所有虚拟机的访问。虚拟化技术可以扩大硬件的容量，简化软件的重新配置过程。中央处理单元（CPU）的虚拟化技术可以利用单 CPU 模拟多 CPU 并行，允许一个平台同时运行多个操作系统，并且应用程序都可以在相互独立的空间内运行而互不影响，从而显著提高计算机的工作效率。

随着云计算技术发展的日益成熟，虚拟化作为基石的作用也日趋明显，尤其体现在提高云计算平台可靠性方面。虚拟化技术之所以能够增强云计算平台的可靠性，主要是因为其具有以下几种机制。

① 服务器整合。

将原来独立的服务器通过虚拟 VMM 合并到同一个逻辑服务器。首先，服务器整合增加了功能部件的复用度，降低了硬件的成本，提高了系统的负载能力，并提高服务器的利用率。其次，通过服务器整合有利于实现负载均衡，避免因系统拥塞造成服务中断或降级。

② 隔离机制。

VMM 的引入，一方面实现了操作系统和底层硬件的解耦；另一方面，实现了各个客户操作系统之间的隔离，每一个应用服务运行在自己的客户操作系统之上，

从而实现各个应用服务之间的独立。由于各个应用服务之间的隔离，使得一种应用服务在遭受攻击或者发生故障时不会波及其他应用服务，从而提高了云平台的可靠性和可用性。隔离机制是虚拟化技术提高云计算系统可靠性的主要方法之一。VMM 提供了重构现有软件系统的能力，同时也便于使用新的方法去构建安全系统。将有安全漏洞的某些功能移到虚拟机的外面，使它们与客体操作系统一起运行但又与之隔离，提供了相同的功能但具有更强的抗攻击能力。

③ 系统管理。

借助虚拟化技术，云计算系统在管理上可实现自动化和智能化，包括：自动侦测物理服务器失效、资源预留、虚拟机自动重新启动、智能选择物理服务器等功能。虚拟化技术降低了管理负担，一系列自动化管理在很大程度上避免了资源分配的不合理和调度不当、因物理资源的失效导致系统失效以及人为因素的失误，从而进一步保证了云计算系统的可靠性。

(2) 云计算系统的可靠性分析方法

① 基于云计算架构和运行方式，分阶段建立可靠性模型。

这种方法的关键是在云计算定义和参考架构（如美国国家标准技术研究院 NIST 提出的典型架构）的基础上，分析服务系统的构成及运行过程，提炼出相关要素，构建云计算系统运行原理图，如图 1-8 所示。

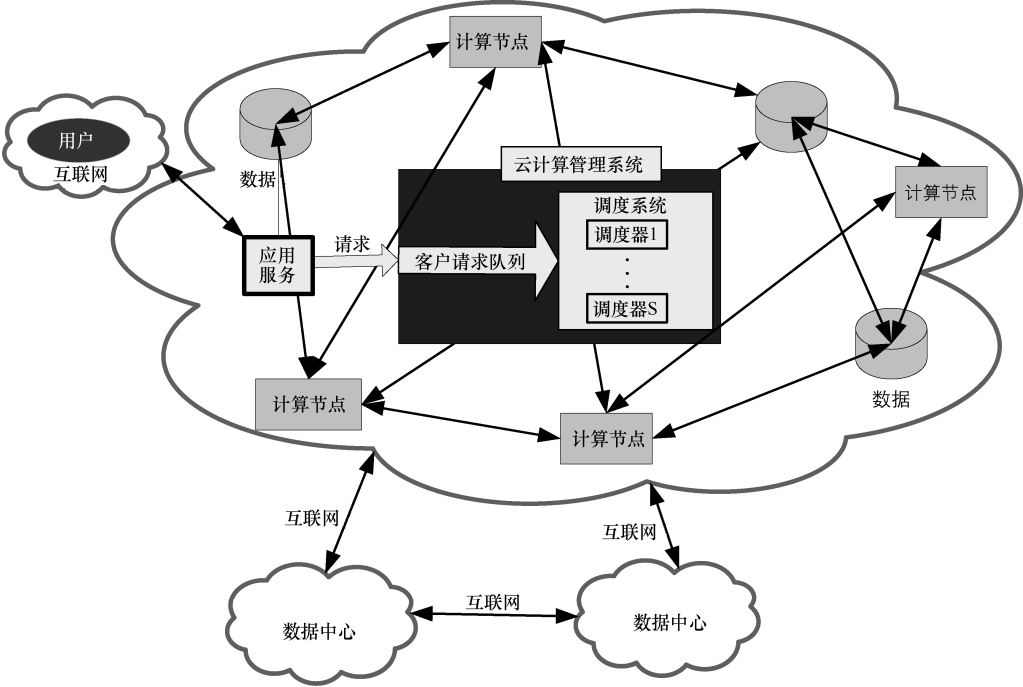


图 1-8 云计算系统运行示意图

云计算服务系统的核心控制部分是云管理系统（Cloud Management System, CMS），其核心功能有 4 个：

- 接收并管理不同客户提出的云计算服务请求。
- 管理云计算系统中的计算资源，包括个人计算机、计算机集群、超级计算机等，统一称为计算节点。
- 管理云计算网络上的存储（数据）资源，包括：各种数据库、公布的信息、统一资源定位器（URL）目录等。
- 调度请求，根据不同的调度算法将请求分解成多个子任务，合理地分配给不同的计算节点。

用户的服务请求通过应用服务接口首先到达云管理系统，CMS 将用户请求划分为多个子任务，如果 CMS 当前的任务队列有足够的空间接纳这些子任务，则子任务可顺利到达调度系统，否则，这些子任务将被阻塞在 CMS 之外，即此次服务请求失败；在任务未被阻塞的情况下（通常需要排队等候，甚至还可能包括一些失效），调度系统顺利接收这些子任务并按照一定的调度算法将子任务调度到各个计算节点，各计算节点根据各个子任务的情况，按照一定的执行顺序或者链路通信交换约束完处理子任务，最终完成用户的服务请求。

在云计算服务系统的运行过程中，可能存在很多故障，导致服务任务无法完成，主要故障模式如下：

- 队列溢出。用户请求以队列的形式到达云计算服务系统，一旦请求数超过最大的允许请求数，这个请求将被丢弃，导致队列溢出的发生。
- 请求超时。云计算服务系统中通常会设置一个时间范围来处理用户请求，如果用户请求在等待被处理的时间超过这个时间阈值，就会产生请求超时错误。超时用户的请求将被丢弃。
- 数据源丢失。在云计算服务系统的管理系统中有一个数据资源管理器（DRM），DRM 为所有的数据资源建立了一个目录，所有的数据资源都要在 DRM 中注册，当数据资源失效或者脱离系统时，该注册信息被删除。
- 计算资源不可用。与数据源丢失相类似的，如果分布式系统中某个计算节点停电或者处于关机状态，而计算资源管理器（CRM）没有及时更新注册信息，调度器又将子任务分派给该计算节点，那么就会导致计算不可用。
- 软件故障。云计算服务系统中的子任务处理都是由具体的软件系统运行在不同的计算机上来完成的，如果软件系统出现故障（如响应超时、内存泄露、读写错误等），整个云计算服务系统也会出现故障。
- 数据库不可达。云计算服务系统中的数据库服务器可能宕机，导致子任务执行过程中访问数据库的时候出现数据库不可达。
- 硬件故障。部署云计算服务系统中的数据库服务，以及其他系统软件、应用软

件的硬件出现过热、电路开、短路等故障，导致硬件不可用，出现硬件故障。

- 人为故障。因人为因素（如错误的操作、配置和维护活动等）引起的故障。
- 环境因素引起的故障。包括机房冷却系统不能正常工作导致环境过热、发生火灾等意外情况引发的云计算系统故障。

依据可靠性的定义，云计算服务系统的可靠性可定义为：云计算系统在给定的条件和规定时间内完成用户请求服务的能力。云计算的任务在于为用户提供服务，如计算服务、存储服务、应用等。系统在尽可能少的时间内处理用户提出的请求，将处理结果反馈给用户，完成一次任务。在该过程中，云计算服务系统的可靠性可定义为：

$$R(t) = (1 - p_B^{(m)}) P_r \{T_{SRT}^{(m)} \leq t\} \quad (1-1)$$

其中：

- $R(t)$ 为云服务系统可靠性，即用户提交的服务请求能够被云计算系统在指定的时间 t 内成功完成的概率。
- m 为用户提交的服务请求在实际执行时被分解成的子任务个数。
- $p_B^{(m)}$ 为用户的服务请求被阻塞（由于请求队列已满）的概率。
- $T_{SRT}^{(m)}$ 为服务响应时间，即从用户提交请求到最终执行完成的时间。
- $P_r \{T_{SRT}^{(m)} \leq t\}$ 为服务响应时间不大于规定时间的概率。

清楚了云计算服务系统的主要故障模式和可靠性定义表达式后，就可以将云计算服务划分为若干个阶段（如任务请求阶段、调度阶段和执行阶段），分阶段构建云计算的可靠性模型，具体方法可见参考文献。

② 仿真方法。

云计算的可靠性仿真一般建立在云计算仿真器的基础上。目前，云计算仿真器很多，其中应用最为广泛的要数 CloudSim。

2009 年 4 月 8 日，澳大利亚墨尔本大学的网格实验室和 Gridbus 项目宣布推出云计算仿真软件，称为 CloudSim。它是在离散事件模拟包 SimJava 上开发的函数库，可在 Windows 和 Linux 系统上跨平台运行。CloudSim 的组件工具均为开源的，它继承了网格仿真软件 GridSim 的编程模型，支持云计算的研究和开发，并提供两个新的特点：一是支持大型云计算基础设施的建模与仿真；二是一个自足的支持数据中心、服务代理人、调度和分配策略的平台。CloudSim 的独特功能有：一是提供虚拟化引擎，旨在数据中心节点上帮助建立和管理多重的、独立的、协同的虚拟化服务；二是在对虚拟化服务分配处理核心时能够在时间共享和空间共享之间灵活切换。CloudSim 平台有助于加快云计算的算法、方法和规范的发展。

图 1-9 给出了基于 CloudSim 云计算的可靠性仿真实现原理框架图。图中英文部分是 CloudSim 的原有架构，中文部分是为实现可靠性仿真增加的功能模块。

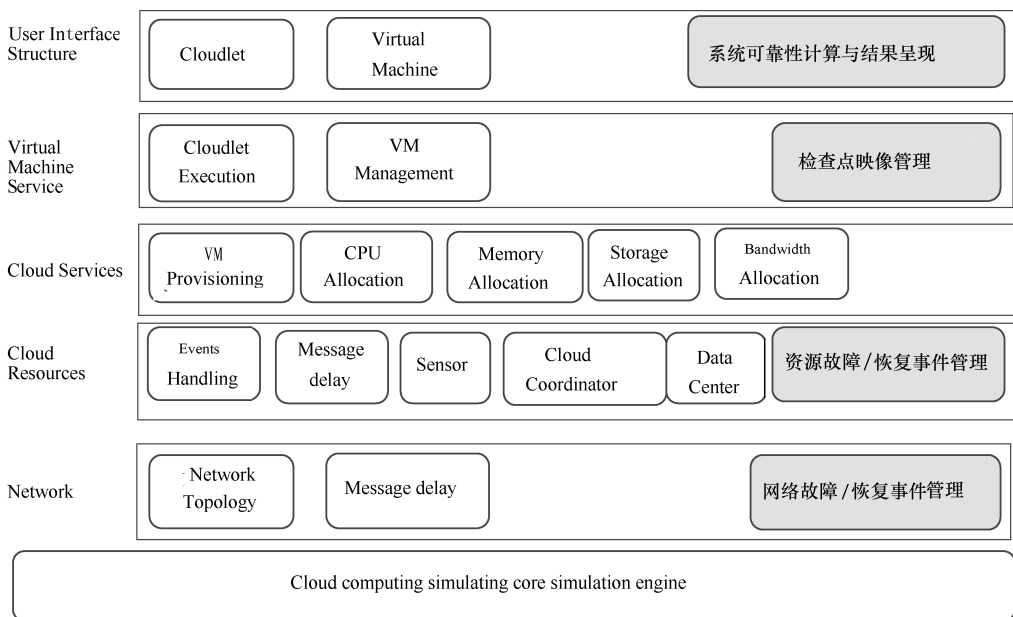


图 1-9 云计算可靠性仿真框架图

一般而言，可以通过增加 4 个功能模块实现可靠性仿真及结果输出，它们分别是：

- 网络故障/恢复事件管理模块（添加在网络层）。用于触发和管理网络故障（如集线器、路由器和链路故障等）及其恢复事件。网络故障事件可以根据某种特定分布（如指数分布、威布尔分布等）触发产生，同时需记录网络故障恢复的时刻。
- 资源故障/恢复事件管理模块（添加在云资源层）。用于触发和管理云计算资源故障（如计算机、存储器、服务器等）及其恢复事件，其功能与上述网络故障/恢复事件管理模块类似。
- 检查点映像管理模块（添加在虚拟机服务层）。该模块拓展虚拟机管理服务功能，重点是在拓展 CloudSim 调度策略的基础上定义检查点调度策略，包括什么时候生成映像、映像的内容及其存储位置等。
- 系统可靠性计算和呈现模块（添加在用户界面层）。获取仿真数据，统计分析并输出可靠性仿真结果，包括可靠度、可用度等。

1.5.8 可靠性与其他质量特性的综合

可靠性是最为重要的质量特性之一，那么，可靠性与其他质量特性的关系如

何？如何实现可靠性与其他质量属性的综合呢？

可靠性与其他质量属性在设计上的融合，是可靠性工程发展的一个重要方向。

可靠性与其他质量属性的融合可以分为两个层次，即：

- 可靠性与其他通用质量特性的综合。
- 可靠性与性能等其他非通用质量属性的综合。

1. 可靠性与其他通用质量特性的综合

如前所述，质量特性是指产品、过程或体系与要求有关的固有特性。装备的通用质量特性，通常包括可靠性、维修性、保障性、测试性、安全性和环境适应性等。而反映不同装备性能的转速、精度、信号覆盖范围、分辨率、射程、亮度等与装备类型或个体密切相关的质量属性，通常被称为专用质量属性。不同装备的专用质量特性一般是不一样的。

随着科技的不断进步和军用、民用装备需求的不断提高，新型装备科技含量和复杂程度越来越高，装备的通用质量特性问题越来越突出，伴随而来的装备使用阶段维修保障问题也越来越多。与战术、技术性能指标一样，通用质量特性是装备研制生产中赋予装备的质量特性。装备通用质量特性是否满足其使用需求，将直接影响到装备效能的发挥，也是关系到军事装备能否形成和保持其战斗力的重要因素。

近年来，装备通用质量特性设计与分析在装备研制中的地位 and 作用已经为广大设计和管理人员所公认，装备通用质量特性工作逐步走上了规范化的轨道。在新型装备研制中，初步改变了以前那种只重视装备技术性能，不重视通用质量特性的状况，使装备通用质量特性研制水平在整体上有了较大的提高，装备通用质量特性工作有了较快的发展。

注意，装备的各个通用质量特性不是独立的，它们之间存在着密切的关联、相互影响。

通用质量特性是一组与时间相关的质量特性，参数大多具有随机特性，对装备的效能发挥都会产生影响。

它们之间相互关联，一个系统或设备不可能永远正常工作，出现故障是不可避免的。可靠性赋予了装备是否容易发生故障的属性；测试性赋予了装备便于确定有无故障和何处发生了故障的特性；维修性赋予了装备便于进行预防性维修和修复性维修的特性，这些属性相互关联。例如，可靠性以故障频度影响维修和保障资源配置（综合保障），测试性以故障检测和隔离的难易影响维修性和保障性。同样，致命故障（可靠性）可能危及人员或财产安全，影响装备的安全性。

可靠性、维修性同为保障性的设计特性，可靠性与维修性共同决定了装备的固有可用度，三者之间的关系可用下式表达：

$$A_i = \frac{MTBF}{MTBF + MTTR} \quad (1-2)$$

式中： A_i ——固有可用度；
 MTBF——平均故障间隔时间；
 MTTR——平均修复时间。

利用一组固定 A_i 可以绘制出一组曲线，如图 1-10 所示。从上式可以看出，固有可用度 (A_i) 仅取决于 MTTR 与 MTBF 之比，图 1-10 给出了描述 A_i 、MTBF、MTTR 相应关系的通用曲线。图中的每一条斜线表示了同样的可用度，从图中不难看出，同样的固有可用度可以有任意种（或多种）MTBF 和 MTTR 的组合，为确定合适的可靠性（MTBF）、维修性（MTTR）提供了权衡的空间，强调提高可靠性时，维修性可以低一些，提高可靠性受到限制时，可以用好的维修性来补偿，所以说可靠性和维修性是两种互补的特性。

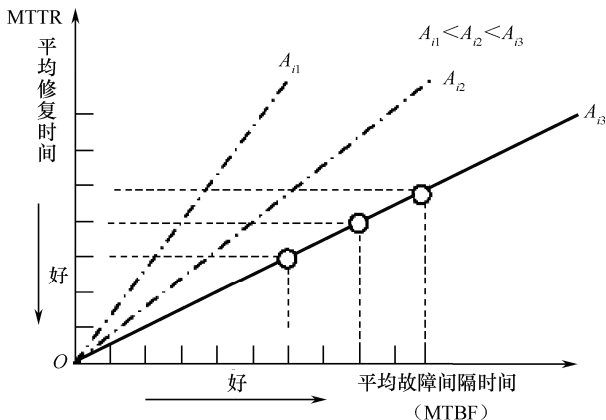


图 1-10 可靠性与维修性的关系及权衡

可靠性与环境适应性之间的关系更为密切。提出合理的环境适应性要求和确保这一要求得到满足的工作贯穿装备寿命期的全过程，其实质就是一个系统的环境工程。环境工程是将各种科学技术和工程实践用于减缓各种环境对装备效能影响或提高装备耐环境能力的一门工程学科，包括环境工程管理、环境分析、环境适应性设计、环境试验与评价等。从可靠性的定义可以看到，可靠性是与使用环境条件密不可分的，图 1-11 列出了可靠性与环境工程的联系。

各通用质量特性的目标是一致的，保持和提高装备通用质量特性的总体目标是提高整体装备的完成任务率，最大限度地发挥其效能。

因此，做好装备通用质量特性之间的权衡分析至关重要。只有将可靠性与其他通用质量特性综合，将它们作为影响装备效能的因素整体加以考虑，才能达到预期的效能目标。

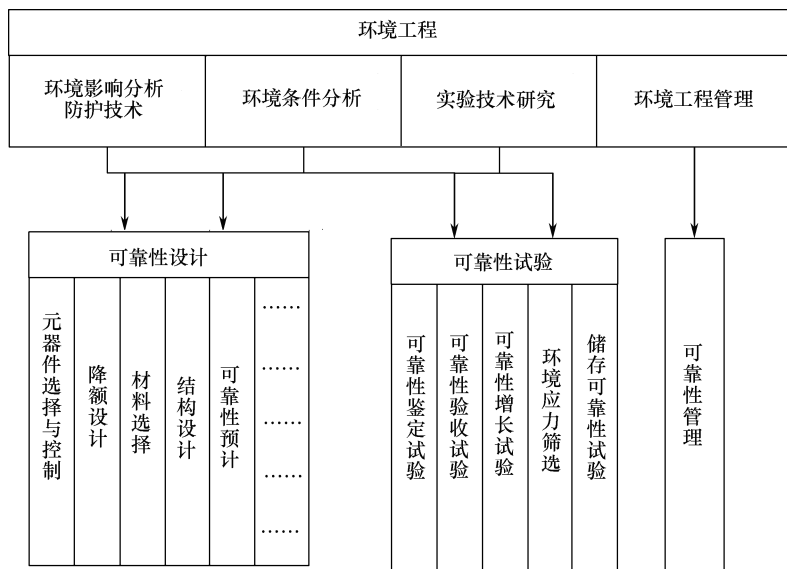


图 1-11 可靠性与环境工程之间的联系

举例来说，如果只是片面强调可靠性，而忽略了测试性、维修性和保障性，很可能会出现不轻易发生故障，一旦发生故障，就难以定位故障、维修困难或维修备件不足等情况。反之，片面强调维修性，不注重可靠性，会造成装备经常发生故障的局面，尽管容易维修，但无疑会严重影响装备正常执行任务。通用质量特性工作覆盖装备的全寿命过程，通用质量特性是在论证中提出，在设计中落实，在研制生产中实现，在使用中发挥、保持和提高的。

通用质量特性工作要靠标准来规范。装备质量特性工作是一项技术性、政策性很强的工作，涉及可靠性、维修性、保障性等具体专业技术，涉及广大的装备承制单位和使用人员，需要统一制定、颁布相关标准予以规范。

通用质量特性水平的形成和提高，需要以关键技术攻关和试验验证为基础。通用质量特性的形成和提高，需要通过一系列的设计、研制工作才能完成，一些重要通用质量特性指标甚至需要通过关键技术攻关才能实现。通用质量特性水平能否达到设计要求，还必须通过试验手段来进行验证，通过使用才能确认。

随着科学技术的发展，为了使装备具有更强大的功能，内部集成化程度越来越高，系统越来越复杂，由此带来的通用质量特性相关问题越来越突出。能否对装备系统实施全特性、全系统和全过程管理，是制约装备发展的主要因素之一。

在军民两用市场需求迫切的新形势下，装备通用质量特性工程将不断向信息化、自动化、综合化、智能化、实用化、仿真化和工具化等方向发展。

- 信息化是新军事变革的本质和核心，也代表了装备通用质量特性工程的发

展趋势。装备通用质量特性工程信息化是实现装备信息化建设的重要领域。利用数字化通信、网络传输等信息技术来完善通用质量特性管理、加快装备通用质量特性的信息系统建设,已成为装备通用质量特性工程发展的必由之路。

- 自动化是通用质量特性发展的另一个趋势。随着计算机辅助技术的日益广泛应用,以计算机为中心的通用质量特性设计与分析自动化将进一步改善装备通用质量特性设计和分析的质量,缩短研制周期,提高通用质量特性水平。通用质量特性管理自动化将大大提高装备的通用质量特性管理效率,通用质量特性信息收集和处理的自动化将提高信息收集速度和精度,从根本上解决通用质量特性的信息问题,最终提高装备通用质量的特性水平。
- 综合化。一是指标体系的综合化,即用综合指标来表征装备的通用质量特性;二是工程体系的综合化,即通用质量特性设计分析综合化、可靠性试验综合化、软硬件可靠性分析综合化、通用质量特性信息综合化。
- 智能化是装备通用质量特性管理和设计分析的专家系统,用于帮助设计师和可靠性工程师设计更加可靠、易保障而且费用更低的装备;通用质量特性设计人员培训专家系统用于培训新装备设计及维修的通用质量特性人员,提高培训质量和效率。
- 实用化。在下一代的装备发展中,诸如 FMECA、FRACAS、FTA、高效环境应力筛选、研制与增长试验、高加速寿命试验、健壮设计技术、PHM 技术等一批高效实用的通用质量特性技术,将会得到进一步重视和发展,新的实用技术也将出现。
- 仿真化。建模、仿真及虚拟现实技术将成为推动通用质量特性发展的一项重要技术,不仅可用于通用质量特性的指标论证、方案权衡、分析与设计,还可用于通用质量特性的试验验证与评价,既可大大提高设计与分析的精度,又可缩短研制周期。
- 工具化。各类通用质量特性工具日臻成熟,且向集成化、协同化、智能化方面发展。

2. 可靠性与性能等其他非通用质量属性的综合

可靠性与性能的综合问题一直是可靠性领域的热点问题,也是可靠性与其他专用质量特性综合的最为典型问题。长期以来,可靠性设计与产品(性能)设计脱节(一般滞后于产品设计),形成事实上的“两张皮”现象,一直为国内工程界所诟病。

产品的可靠性是设计出来的,如果不能将可靠性设计到产品中,事后无论如

何检验、如何采用补偿措施，都是杯水车薪，很难从根本上解决问题。因此，开展可靠性（这里可理解为广义的可靠性）与性能综合设计、同步设计、并行设计，将可靠性预测、分析发现的设计缺陷以及有效的预防措施及时反馈到设计师系统，及时改进有缺陷的设计，才能实实在在地提高产品的可靠性，进而设计出高可靠性的产品。

美国航空航天局（NASA）在 2006 年发布 NASA/CR-2006 Model-Based Safety Analysis（基于模型的安全性分析）技术规范，开展基于产品设计模型的可靠性、安全性分析技术研究和航空航天领域应用，取得显著成效。

欧洲空中客车（Airbus）自 2003 年起，组织实施了 ESACS、ISAAC、VIVACE、SPEEDS、MISSA（均为项目代号）等一系列基于模型的故障传播、设计仿真、虚拟测试、诊断分析和数据交换等可靠性、测试性、安全性方面的研究与工程实践，并开发相应的软件平台，极大提高了可靠性、测试性和安全性设计分析效率，初步实现产品设计与通用质量特性设计的一体化。

我国学者近年来也开展了可靠性与性能综合技术研究，取得一定的进展。

随着计算辅助设计（CAD）、辅助制造（CAM）和辅助工程（CAE）的发展深入，基于产品的数字样机，采用形式化建模技术，开展辅助可靠性预测、分析、仿真验证，以及与性能、费用等因素的综合权衡，已经成为目前的一个研究热点和技术发展趋势，相信在不久的将来会成为现实，并且技术上不断成熟，能够得到较普遍的应用。

1.5.9 基于失效物理的故障预测与健康管理

1. 失效物理简述

在讨论失效物理（Physics of Failure, PoF）概念前，还有两个与失效有关的重要概念需要明确，即失效模式与失效机理。

- 失效模式（Failure Mode）：失效的表现形式。
- 失效机理（Failure Mechanism）：引起失效所发生的微观物理、化学变化等内在原因。失效模式与失效机理之间的关系就好比病症与病理。

失效物理是一门研究产品失效机理的学科，失效物理分析的目的在于以可靠性技术为理论基础，引入物理与化学的思考和方法，说明构成产品的零件或材料的失效机理，并以此作为消除或减少失效发生原因的依据，以提升产品的可靠性。通过对失效样品的破损分析，有助于发现对失效敏感的特性参数，了解零件、材料的失效数学模型（Failure Model）及退化模式（Degradation Pattern）等失效机理信息，进而建立寿命与应力间关系的数学模型，这些成果应用于材料与元器件层次，可以

开发潜在缺陷的检测技术，规划实用的筛选与非破坏检测方法，开发加速寿命试验（Accelerated Life Test）、过应力试验（Overstress Test）等寿命试验与测量工作，失效物理分析流程如图 1-12 所示。

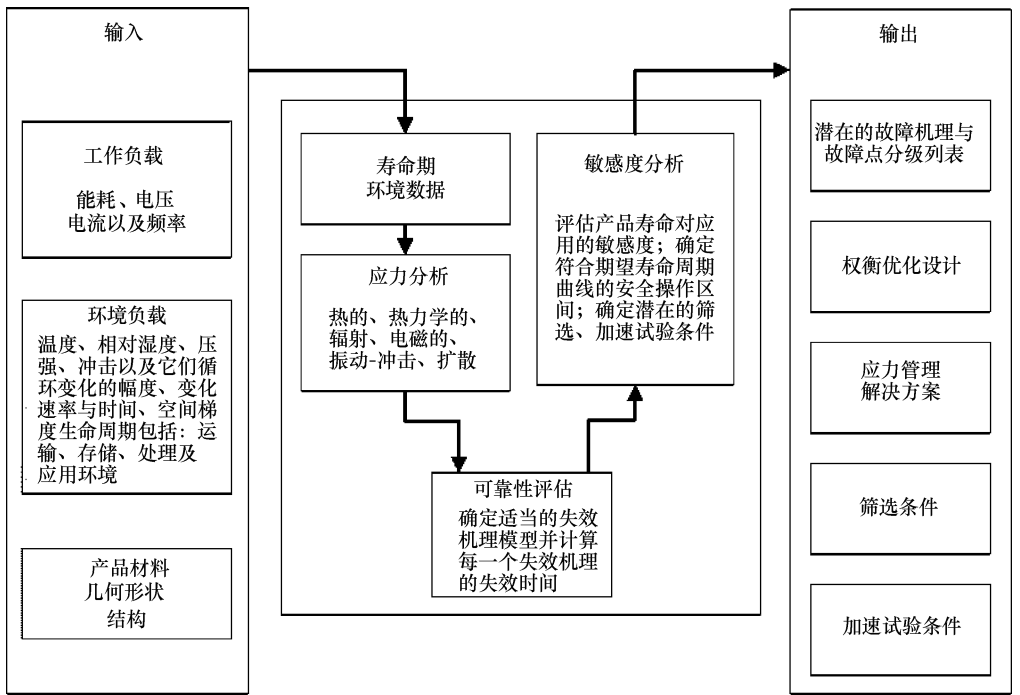


图 1-12 失效物理分析流程

产品在研发、生产、储存、使用等各个阶段都可能发生失效，认真地考察各阶段上的失效形态，并以此为出发点来开展失效分析工作，并从观测到的失效模式进而探究失效的诱因——工作应力、环境应力和时间等，从中揭示出失效发生的本质原因与过程，即失效机理。

失效物理从物理、化学等微观结构的角度出发，研究材料、零件（元器件）和结构的故障机理，并分析工作条件、环境应力及时间对产品退化或故障的影响，为产品可靠性设计、使用、维修以及材料、零件（元器件）和结构的改进提供依据。由于器件的失效行为与失效物理有着极为密切的关系，而失效分析又是可靠度技术的核心工作之一，因而又有人将失效物理称为可靠性物理（Reliability Physics）。

可靠性研究始于对产品失效的统计分析，而失效物理分析方法是从实体验证的立场追究失效原因，提出本质上的改善方法。失效物理所涵盖的内容也不只是狭义的物理学，还涉及材料学、冶金学、金相学、物性论、化学、电气、机械等固有技术领域，以及环境科学、规划技术、失效破损分析、统计分析等学科。



失效物理分析的目的在于研究失效发生的原因、过程与机理，常见的分析方法有：

- 直接调查失效本身。
- 观测失效前的应力状态或失效的诱因，利用非破坏性检测技术，调查容易发生失效部位的特性与状态，然后研究这些项目与实际失效的关系。

失效物理分析是一种探讨失效机理的技术，主要是以找出失效的真正原因为目的。目前，失效物理在失效分析中扮演着极为重要的角色，透过传统物理与化学的思考和方法，了解零件或材料的失效机理，进而消除或减少失效发生原因，使零件或材料具备高可靠性。其主要作用有：

- 通过分析，确定产品的失效模式和机理，通过采取纠正或补偿措施消除失效隐患，从根本上解决产品失效问题。它是产品故障归零管理的一种重要辅助手段。
- 为加速试验、施加应力、构建剖面和评价试验结果等提供理论支撑。
- 其是产品故障预测的一种重要手段。通过分析产品的失效机理，找出其失效规律，可有效预测产品的寿命或故障时间。

2. 故障预测与健康管理

故障预测与健康管理（PHM）是近年来兴起和发展的可靠性方面的新领域。PHM 利用先进传感器和通信技术，借助各种算法、模型和手段，实时监控和管理装备的健康状态，预测装备的寿命或可能的故障时间，并根据预测采取有效的故障预防或减缓措施，消除故障隐患，以实现装备的持续稳定运行。

PHM 系统的功能主要包括：

- 故障检测与隔离。装备具有良好的测试性和机内测试（BIT）能力，能够准确进行故障检测，并有效隔离，指出故障部位。
- 信息采集、传输、存储、管理、融合和推理。通过传感器采集装备各层次产品（部件和分系统等）的相关数据，通过传输、存储、管理，利用专家系统进行推理，借助系统模型、相关信息融合技术，实现增强的诊断功能，精确地检测和隔离系统、部件、子单元的故障或失效状态，超越传统装备的测试性和 BIT 能力。
- 故障告警。提供有效的故障自动预警功能，在故障发生前的适当时刻向系统监控者或操作者提供预警信息。
- 部件寿命和性能降级趋势跟踪。跟踪、积累装备的寿命消耗情况，或者对产品的性能降级实施持续跟踪。

- 故障预测及残余使用寿命预计。包括早期检测部件或子单元的故障症状或初始故障状态，并根据材料的实际状况预计剩余使用寿命；预计在部件初始故障状态向最终失效发展过程中的任一时间的剩余使用寿命。
- 状态管理与辅助维修保障决策。根据装备实际的和预计的材料状况进行维修、供应，以及其他维修保障活动的辅助决策，包括在装备存在功能降级的情况下，能够保证在最大程度上完成装备被赋予的任务。

PHM 使得原来由事件主宰的维修（即事后维修）或按时间实行的维修（即定期维修）向基于状态的维修（CBM，即视情况维修）转变，即从传统的基于传感器的诊断转向基于智能系统的预测，由反应式维修转向先导式的预先维护。

当前 PHM 技术的发展主要体现在：以系统级集成应用为牵引，提高故障诊断与预测精度、扩展健康监控的应用对象范围，支持 CBM 与自主保障（AL）的发展等方面。

PHM 系统的预测能力是其与以往系统的维修诊断系统的最主要区别。PHM 智能诊断系统能够检测系统的各种变量（如振动模式、温度、压力、电应力等）的关系或水平上的微小变化，并且根据经验积累形成的专家系统，判断是否为故障的先兆，准确预计未来某个时刻可能发生的故障，即让装备自动监测、诊断自身的健康状况，并利用专家系统实现事故发生前的预测，给出优化的装备维护方案。

预测是 PHM 系统的关键技术之一，目前国内外的故障预测方法可以归纳为以下 3 类。

- 监测失效征兆，预测故障。将传感器嵌入被测对象，对其失效征兆进行监测，搜集和分析与失效密切相关的参数（如性能参数、退化参数等）。利用产品的关键参数变化来预测故障，如利用焊接件焊点的电阻变化来预测电子产品的残余寿命、利用动态功耗来预测电路故障。
- 设置预警电路（Canary Devices）预测故障。通过在产品中设置预警电路来诊断与预测故障，其基本原理大致如下：使预警电路比产品正常使用的电路具有更高的失效率——通过减少预警电路的线路直径增加其电流密度，使其热量比正常使用电路产生的热量大，随着时间的推移，热应力增加到一定程度使预警电路先于电子产品发生失效，从而提供故障的早期预警。例如，美国 Rockwell 公司对于具有低循环疲劳特性的焊接件和腐蚀件，利用产品中的预警电路进行故障早期诊断，Ridgetop 集团对电子产品的主机电路设置预警电路来提供故障预测。
- 建立累积损伤模型预测故障。基于物理失效和原位监测对产品实际的寿命



周期载荷进行搜集与分析,建立累积损伤模型,评估产品的退化趋势。寿命周期载荷是指产品寿命期内所承受的全部外部载荷条件。通过在产品中嵌入一组传感器来检测影响产品可靠性的载荷,应用建立的复合载荷累积损伤模型,可预测产品的参与寿命。例如,马里兰大学运用基于物理的损伤模型处理监测参数,监测寿命消耗,计算累积损伤,评估电子产品的残余寿命;Impact 技术公司将传感器参数与基于物理的损伤模型相结合,对 GPS 等系统进行寿命损耗监测。

此外,一些新的预测方法也在探索中。例如,NASA 在航天飞机中使用故障检测算法(包括高斯混合模型、隐马尔可夫模型、卡尔曼滤波、虚拟传感器等)来检测产品异常状态;史密斯航宇集团在飞机和直升机子系统中综合利用离群值分解、主成分分析和神经网络进行非线性多元分析和异常状况检测。

3. PHM 面临的挑战

尽管 PHM 技术发展迅速,并且取得一定的应用成果,但目前仍然面临诸多挑战,主要表现在以下几方面。

(1) 基于物理的损伤模型

PHM 最大的难点和挑战来自损伤模型。大家都知道,产品的失效是由于物理、电、化学、机械等应力综合作用的结果。损伤模型的建立一般基于失效物理(PoF)分析。确定失效机理除了选用合适可用的失效模式外,还要结合潜在的失效模式与失效原因进行分析。失效机理一般可分为过应力机理和磨损机理两种典型形式:过应力失效机理一般用于单一载荷(应力)引起的失效;磨损机理一般用于多种应力条件引起的失效。

基于物理失效的方法进行可靠性预测的挑战主要来自两个方面:

① 产品及其故障模式的多样性。

由于产品品种繁多,其故障模式各异,如何找出各种产品与其寿命相关的关键故障模式和原因,并进一步探索发现相关的影响其寿命的关键因素及其规律,从而建立起基于失效物理的产品损伤模型,一直是 PHM 领域的研究热点和重大挑战。这是影响 PHM 技术应用广泛性的重要原因,也是 PHM 一直想要取代传统的基于统计的可靠性预测,但却无法实现的根本原因。目前,基于失效物理的预测和基于统计的可靠性预测技术同时共存。笔者认为,两者用不同方法预测产品的可靠性,互为补充和印证,对可靠性技术的发展和实践未必不是一件好事。一般而言,PoF 方法适用于独特的个体,对那些失效机理明确,已建立起损伤模型的重要产品,采用 PoF 方法;而对那些失效机理不明确,未有损伤模型,且有大量的试验和现场数据的产品,采用基于统计的可靠性预测技术无疑是正确的选择。基于统计的可靠性预

测适用于有一定数量的批次产品。

② 残余寿命预测的不确定性。

在应用损伤模型进行产品的故障预测时,存在不确定性,但不确定性分析面临诸多挑战。首先,不确定性的来源有多种,包括测量设备的不确定性、参数不确定性、失效评价标准不确定性等。其次,缺乏有效的定量评估不确定性的模型,采用不同的不确定分析模型时评价结果的差异很大,对不同模型的有效性很难给出客观的评价。残存寿命预测的不确定性会给维修保障决策带来困难。例如,当预测的残存寿命区间过宽,会使得维修保障决策者难以确定在哪个时刻进行维修保障;反之,如果过窄,会增加错过维修保障时机而发生故障的风险。针对故障预测的不确定性,如何进行风险-收益分析,实现容忍不确定性的保障决策是必须直面的挑战。主要应对措施包括:研究混合及智能数据融合技术,加强经验数据与故障注入数据的积累,提高诊断与预测置信度;不断寻求高信噪比的健康监控途径;研究灵巧、健壮传感器,提高数据源阶段的精度等。

(2) 系统性能的门限值

一个系统或产品一般由多个相互影响的部分组成。某一性能参数的微小变化,可能会导致其他参数的变化,因此很难为每一个参数设定固定的门限值。在设定系统性能门限值时,若不考虑多重参数的交互作用,可能会导致预测的不正确,进而引致错误的维修保障决策。在产品寿命周期内,遭遇的实际环境与操作条件也可能与设定的寿命环境剖面存在差异,在这种情况下,设置门限值可能不适合实际工作环境下的产品。因此,难以建立正确的系统性能基线。

(3) 间歇失效的预测

间歇失效指的是不能鉴定且未来不能复现的失效。由于无法复现,很难找出其真正的失效模式和失效机理。显然,现有的基于物理的损伤模型不能有效预测间歇失效。如何让 PHM 系统预测间歇性故障,将面临巨大挑战。

(4) PHM 技术与被测对象的集成

对新研制的装备而言,在 PHM 系统集成应用方面,如何实施并行工程,将 PHM 系统与被监控装备同步设计、同步生产和同步验证,是需要优先考虑的问题。

将 PHM 集成到已有的传统装备中也将面临挑战,主要表现在,PHM 系统包括传感器、电子设备、计算机和软件,大部分是商业货架产品。这些商业货架产品常常对操作环境、输入参数和使用条件具有特殊要求,难以利用兼容方式综合各种技术,需要克服诸多集成障碍。另外,将 PHM 组件植入已有的传统装备时难免会对装备的性能、布局、重量、电应力和环境应力等带来影响,需要科学综合、权衡分析。

1.5.10 无铅焊点的可靠性

半个多世纪以来,由于锡铅钎料价格低廉,性能优良,已广泛用于电子电气产品。由于电子垃圾的填埋,污染土壤及地下水源,导致严重的环境问题,因此,采用无铅焊料成为必然的选择。

欧盟电子电气产品环保指令的立法和实施,促使电子产品进入无铅制造时代,全球无铅焊接技术的应用成为势不可当的潮流,包括焊料合金的选择、评价、工艺设计以及结构设计等。

目前,欧盟电子电气产品环保指令主要包括 3 个,即:

- WEEE (2002/96/EC) 针对减少废弃物和产品寿命终了再循环的指令。
- RoHS (2002/95/EC) 限制和禁止使用铅等 6 种有毒有害物质的指令。
- EuP (2005/32/EC) 要求产品采用绿色设计与制造,提高产品能效的指令。

2006 年我国由原信息产业部等七部委联合发布《电子信息产品污染控制管理办法》,实际上就是我国的 RoHS 指令,涵盖了家电、通信设备、计算机、电子电气工具和专用设备、仪器、仪表、元器件和专用材料等众多电子电气产品。

RoHS 指令对电子电气产品制造业的冲击很大,为了适应指令的要求和扩大产品出口的技术要求,无铅替代已为大多数企业所接受。学术界一直关注无铅替代问题,从理论和技术方法上为无铅替代做准备。

虽然无铅技术已为企业广泛接受,无铅替代在材料和生产工艺上的变化却带来一系列可靠性的新问题。电子产品中焊点的可靠性直接关系到产品的使用寿命,但目前无铅焊点的可靠性还存在诸多问题和争议。

国内外对无铅焊接的可靠性研究仍是一个发展中的课题。针对焊点可靠性的研究大部分都是基于含铅钎料,而对无铅钎料的研究主要集中在钎料合金成分、钎料机械、热疲劳性能,以及无铅钎料带来的工艺和可靠性问题等方面,对无铅钎料引起的焊点可靠性问题研究较少,综合考虑热循环和随机振动加载下的焊点可靠性研究更少。不同材料、不同焊点形状的焊点失效模式不尽相同。了解焊点失效模式对正确使用元器件、改进工艺以及可靠性分析十分重要。焊点失效主要应考虑焊接材料和工艺两方面:

- 焊接材料方面。电子封装领域使用的焊料有着很严格的性能要求,无铅焊料也不例外,不仅包括电学和力学性能,还必须具有理想的熔融温度。影响焊料可靠性的性能包括其导电性、导热性、热膨胀系数、剪切性能、拉伸性能、抗蠕变性能、疲劳性能、抗氧化和腐蚀的能力以及形成的金属间

化合物影响等。

- 焊接工艺方面，与传统的含铅工艺相比，无铅化焊接由于焊料的差异和工艺参数的调整，必然会给焊点可靠性带来一定的影响：首先是目前无铅焊料的熔点较高，一般都在 217°C 左右，而传统的锡铅（SnPb）共晶焊料熔点是 183°C ，温度曲线的提升随之会带来焊料易氧化及金属间化合物生长迅速等问题；其次是由于焊料不含 Pb，焊料的润湿性能较差，容易导致产品焊点的自校准能力、拉伸强度、剪切强度等不能满足要求。

鉴于无铅化焊点可靠性方面目前仍存在许多问题，有必要对此进行深入的分析、研究。

从无铅焊点可靠性实验验证，以及利用有限元分析对焊点力学性能、疲劳寿命方面来研究无铅焊点可靠性，对电子产品无铅化实施具有重要的理论价值和实际意义。

在电子电气产品组装中，钎焊接头起着电连接和机械连接的双重作用。由于连接接头材料的热膨胀系数差别，环境温度循环或功率循环使电子组装焊点产生热疲劳或热力疲劳，从而引发钎焊接头的损伤、裂纹萌生与扩展，逐步丧失电连接或机械连接作用，而且焊点电阻的增加还可能引起电信号的失真。有的电子产品，在服役过程中还可能经受振动、冲击或意外跌落，加速钎焊接头的失效。

失效方式对疲劳模型的建立有着重要影响。组装结构的疲劳失效是在应力应变的循环作用下发生的永久损伤。电子产品在长期服役过程中的失效，可发生在应力远低于材料抗拉强度或屈服极限的条件下。疲劳失效通常包括裂纹的萌生和扩展两部分，对实际的电子组装产品，往往很难监测这一过程。目前已研究出很多钎焊接头疲劳行为的预测模型，并在各自适用的范围内得到应用。

在电子组装设计中如何运用疲劳模型进行寿命预测，是企业十分关心的问题。为了应对电子产品市场的快速变化，不断设计出新的组装产品，对新产品设计工程师来说，就需要一种简便快速的方法确定疲劳寿命，如根据经验预测疲劳寿命，只需要知道温度范围及循环频率，按照经验模型计算加速因子，然后由加速因子获得威布尔统计失效分布。这个方法不需要有限元计算或建模，也不需要复杂的曲线拟合或应变迟滞曲线估计，优点是疲劳寿命预测快，缺点是没有考虑显微组织及失效机制的影响，也忽略了钎焊接头几何形状的影响。另一种方法是有限元分析，采用合适的本构关系，疲劳计算模型可以是二维或三维的，二维模型的计算速度快，模型求解时需要材料的应力应变关系或迟滞曲线。

目前的寿命预测模型基本上都是针对 SnPb 钎料，这些模型向无铅过渡尚需大量工作。需要深入了解无铅组装的失效模式和机制、无铅钎料的热力本构关系，还需要可靠性试验数据的积累，建立实验确定的循环失效寿命与有限元模拟分析结果

的对应关系。最近的研究表明,采用锡银铜 (SnAgCu) 等无铅钎料组装的疲劳性能,是否优于 SnSb 钎料还很难说,取决于组装的结构类型和服役条件。

无铅焊点可靠性的研究方法 with 锡铅 (SnPb) 焊点相似,早期钎焊接头的疲劳模型建立在热循环试验的基础上,模型的应力应变数据由应变片测量获得,然而随着钎焊接头尺寸的不断减小,要通过实验获得疲劳寿命计算所需应力应变数据非常困难,另外,在实验中只能测量出焊点表面或平均的应变值,而且必须制作适合的试件,实验设备还得满足很高的精度要求。目前国内外研究人员在预测分析焊点可靠性寿命时,主要在黏性弹力学、断裂力学和弹性力学等理论上,采用有限元数值模拟的方法实现,研究表明有限元数值分析方法与可靠性实验得出的结果相差较小,可以用有限元数值分析方法来代替实验方法。因此,在试验条件难以达到的情况下,可用有限元仿真的方法代替可靠性试验方法,对焊点进行可靠性研究。通过可靠性强化实验分析验证焊点可靠性,用有限元仿真的方法进行失效模式验证,并在综合加载条件下进行无铅焊点的寿命预测将成为焊点可靠性研究工作的发展趋势。

焊点在微电子封装产业中起着举足轻重的作用,相关设计、工艺均应引起充分重视。积极优化焊接工艺、找出失效模式、分析失效机理、提高产品质量和可靠性水平,对电子封装产业均有重要的意义。

无铅焊点的可靠性问题主要来源于:焊点的剪切疲劳与蠕变裂纹、电迁移、焊料与基体界面金属间化合物形成裂纹、Sn 晶须生长引起短路、电腐蚀和化学腐蚀问题等,需要从设计、材料、工艺和使用环境等方面消除影响无铅焊点可靠性的不利因素。

1. 设计方面

主要是印制电路板 (PCB) 的合理设计问题,如焊盘设计不合理、发热量大的元件密集分布、相邻高大元件在回流焊时产生“高楼效应”、形成热风冲击等,因此,在 PCB 设计时,应充分考虑散热因素,将大功率元件置于易散热的位置,并且避免大功率器件的过度集中。

2. 材料方面

焊料的选择极为重要。目前,大多采用锡银铜合金系列,液相温度是 $217^{\circ}\text{C} \sim 221^{\circ}\text{C}$,这就要求再流焊具有较高的峰值温度,如前所述会带来焊料及导体材料(如铜箔)易高温氧化、金属间化合物生长迅速等问题。研究表明,界面上的金属间化合物是影响焊点可靠性的一个关键因素。过厚的金属间化合物层的存在会导致焊点断裂、韧性和抗低周疲劳能力下降,从而导致焊点的可靠性降低。同时焊料和助焊剂的兼容性也会对焊点的可靠性产生非常大的影响。焊料和助焊剂各成分之间不兼容会导致附着力减小。此外,由于热膨胀系数不匹配,又会加快焊料周期性的

疲劳失效，因此要特别注意选择兼容性优良的焊料和助焊剂，才能耐受住无铅再流焊时的高温冲击。

3. 工艺方面

在 SMT、MCM 制作工艺过程中，通常会遇到诸如焊料储存温度不当、焊盘焊料不足、再流焊温度曲线设置不当等问题。就无铅焊接而言，再流焊工艺温度曲线的优化至为重要，优良的工艺既可保证形成高可靠性的焊接，又能保持尽可能低的峰值温度。

4. 使用环境方面

对于汽车和航空用电子产品，在一些场合要求器件在大于 100°C 的环境下长期工作，这就要求焊点具有更高的强度和组织性能的稳定性；在极地环境和空间探测活动（如登月和火星探测等）中，电子器件在低温（ 0°C 以下）或深冷低温（ -150°C 以下）的环境下工作或服役，此时，对电子封装无铅焊点的低温性能和可靠性有较高的要求。电子产品在使用过程中，器件的不同工作状态和环境温度的周期性变化，会使焊点处于持续的温度循环中。由于 PCB 和器件热膨胀系数（CTE）不匹配，焊点在升降温的循环过程中承受反复的应力应变将导致焊点中裂纹的萌生和扩展，最终导致焊点失效。因此，在不同环境下使用的 PCB，必须有针对性的耐环境设计。

无铅化技术已经日趋成熟，但是在无铅化进程中还存在一些悬而未决的问题，如焊点的剪切疲劳、蠕变问题、虚焊现象、焊点热疲劳的主要变形机制、焊点的显微结构对焊点的疲劳行为的影响与作用机制等，都有待进一步研究。

由于无铅替代在材料和生产工艺上的变化，积累的经验 and 数据有限，对无铅产品的可靠性问题仍待进一步研究和加深认识。无铅替代的初期，可能更关心钎焊工艺、焊点缺陷的检测与评价，以及相关检测平台的建设和检测标准的建立。但用户更关注产品运行的长期可靠性，所以必须从理论和技术上，解决无铅替代引发的可靠性新问题，建立产品可靠性和寿命的预测模型、求解方法和可靠性评价的技术规范，最终解决电子电气产品无铅替代及其可靠性问题。

1.5.11 纳米技术的可靠性

在 1981 年扫描隧道显微镜发明后，诞生了纳米技术（nanotechnology），它的最终目标是直接以原子或分子来构造具有特定功能的产品。纳米技术也称毫微技术，是用单个原子、分子制造物质的科学技术，研究结构尺寸在 $0.1\sim 100\text{nm}$ 范围内材料的性质和应用。纳米科学技术以许多现代先进科学技术为基础，它是现代科学（混沌物理、量子力学、介观物理、分子生物学）和现代技术（计算机技术、微电子和扫描隧道显微镜技术、核分析技术）结合的产物。

从物理限制和技术实现两方面来看，传统的互补金属氧化物半导体（CMOS）集成电路正在迅速接近其尺度极限。新兴的纳米电子器件技术和其所对应的纳米电子结构技术被认为可以在短期内补充甚至在未来替代 CMOS 技术。

纳米电子系统的设计和制造面临一系列新的问题，如极高的器件缺陷密度、局部互连限制、新的逻辑表达形式，以及运行时的较高瞬态错误率等。纳米电子器件极小的尺寸和严重的不可靠性，成为当前电子科学和工程所面临的严峻挑战。

目前，可靠性领域正面临与纳米电子相关的两方面挑战：失效机理的识别、纳米电子系统的可靠性设计问题。

- 失效机理的识别。由于几乎每天都有新的纳米电子产品出现，对这些设备的失效机理以及失效背后可能的原因显然无法立刻了解。依据人类现存的知识，显然常常无法识别出确切的故障。事实上，大家经常会遇到许多找不到故障原因的纳米产品失效，也没有充分信心制造出十分可靠的纳米产品。
- 连接线的短路（如不合适的蚀刻和绝缘结构）和开路（如纳米线路的电子迁移）造成了传统电子产品的大多数失效。新材料、大量的连接、更高的功能速度、新的线路设计规则或其他因素是否会导致更多与开路和阻抗变化相关的失效呢？识别纳米电子失效机理会对寿命实验策略的正确确定、高加速应力筛选（HASS）、提高可靠性的筛选、可靠性预计、保质期限和条件，以及很多其他过程产生冲击。现在理解纳米电子失效机理所遇到的障碍要比以前多了，因为不能确定大多数基于过去技术的知识对于纳米产品的可靠性分析是否有效。对于系统设计者而言，为了更好地应用纳米设备、设计出更好的容错系统，理解纳米电子的失效机理是至关重要的。

近年来，纳米电子系统的可靠性设计开始成为电子设计自动化和可靠性测试领域一个新的研究热点，研究工作主要集中在容缺陷设计和容错设计两个方面。面对纳米电子系统极高的缺陷密度，为了保证纳米芯片的可用性，未来的纳米芯片设计和制造工业迫切需要有效的容缺陷设计和容错设计技术。

1.5.12 可靠性仿真试验

1. 可靠性试验的发展历程与趋势

可靠性试验技术按其发展历程大致可分为可靠性统计试验、工程试验、加速试验、系统试验和仿真试验等。各种试验技术的发展进程和趋势见图 1-13。

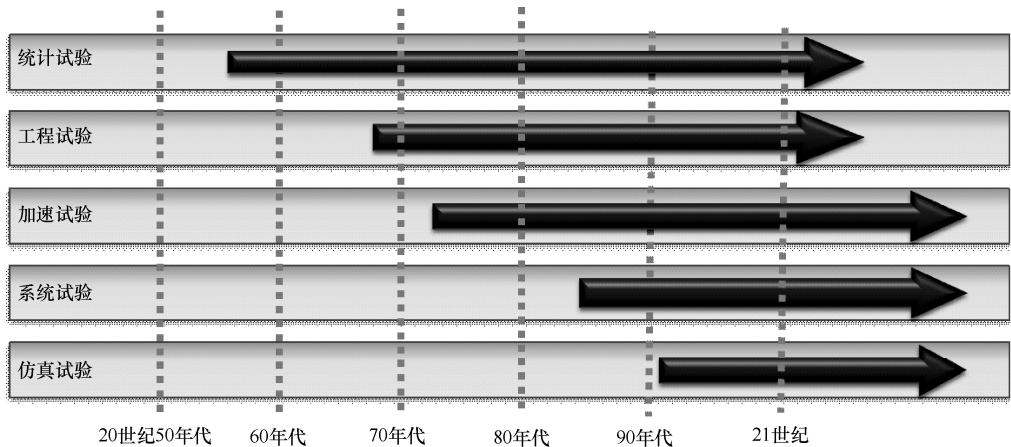


图 1-13 可靠性试验的发展进程和趋势

以美国为例，其标志性的发展情况简述如下。

（1）统计试验

可靠性试验始于可靠性统计试验。从 20 世纪 50 年代开始，美国就开始了可靠性统计试验的研究与实践。

- 1959 年颁发 MIL-R-26667A “电子设备可靠性要求的通用规范”。
- 1965 年颁发 MIL-STD-781A “可靠性试验（指数分布）”。
- 1967 年颁发 MIL-STD-781B “可靠性设计鉴定试验和验收试验（指数分布）”。
- 1977 年颁发 MIL-STD-781C “可靠性设计鉴定试验及验收试验（指数分布）”。
- 1986 年颁发 MIL-STD-781D “工程研制、鉴定和生产的可靠性试验”。
- 1996 年颁发 MIL-HDBK-781A “工程、研制、合格鉴定和生产用的可靠性试验方法、方案和环境”。

（2）工程试验

- 20 世纪 60 ~ 70 年代初期，美国开始采用可靠性研制和增长试验。
- 1977 年颁发 MIL-STD-2068 “可靠性研制试验”。
- 1978 年颁发 MIL-STD-1635 “可靠性增长试验”。
- 1985 年颁布 MIL-STD-2164 “电子产品环境应力筛选过程”。
- 1986 年颁布 MIL-HDBK-344 “电子产品环境应力筛选方法”（定量）。
- 1996 年颁布 MIL-HDBK-2164A “电子产品环境应力筛选方法”。

（3）加速试验

20 世纪 70 年代初，美国开始研究和应用恒定应力加速寿命试验技术，20 世纪

80 年代末,采取可靠性强化试验、高加速寿命试验、高加速应力筛选,20 世纪 90 年代末开始实施基于故障物理的可靠性加速试验。

(4) 系统试验

美国空军的先进战斗机 F-22 和波音公司的波音 777 型民用飞机都建立大型的地面实验室进行系统综合试验。

为了保证波音 777 型飞机在首次试飞前能尽早发现并纠正系统的接口可靠性问题,对飞行操纵系统、航空电子系统等某些关键系统进行了系统级试验,暴露了产品的接口兼容性问题,从而提高了整机的可靠性水平。

(5) 仿真试验

建模仿真技术已成为装备研制中不可或缺的关键使能技术。美国国防部在 DoDD 5000.1 “防务采办系统”中指出,应将“建模仿真—物理试验—模型改进”贯穿于装备研制的全过程。

1985 年美国陆军装备系统分析中心 (AMSAA) 与马里兰大学 Calce 中心合作,对基于故障物理的可靠性技术进行研究,并开发出可靠性仿真软件工具,将该技术和软件工具应用到多军种通用无线电台、布莱得利战车、长弓阿帕奇等装备的电子设备和机械系统中,取得良好效果。

目前,虚拟试验技术已广泛用于国外武器装备的采办过程中,从系统方案论证到使用训练的各个阶段,在降低技术风险、缩短研制周期、降低费用等方面取得可观的效益。例如,美国在研制第四代攻击机 F-35 项目时提出“从设计到飞行试验全面数字化”,其研制周期比 F-22 缩短一半,风洞试验减少 75%,试飞架次减少 40%,定型试验周期缩短 30%。在美军 F-22、F-35 等第四代战斗机的气动载荷计算、油箱方案优化、流场分析等方面都采用了虚拟试验验证技术;美国航空业两巨头波音和洛马公司在竞标 JSF 项目时,除设计新战机外,都建立了虚拟试验验证系统,用于研发和测试新战机,并用于训练飞行员和地勤人员。在两家公司的飞机真正试飞前,已在虚拟系统上进行了数千小时的虚拟试验。

美军最新颁发的防务采办条例 DoDI 5000.2 “国防部采办系统运作”强调:将研制试验与评定、使用试验与评定、建模与仿真工作纳入系统设计和研制工作中。综合协同利用地面试验分析、数学建模、仿真分析和使用试验等试验分析手段,形成以“建模仿真—虚拟试验—物理验证—模型改进”综合试验与评价,贯穿于装备研制生产和使用的全过程。

在导弹武器系统的研制过程中,以虚拟技术模拟飞行试验,替代部分乃至大部分实弹试验,而实弹试验则仅作为一种有效性的验证手段,从而达到在保证武器系统性能的基础上节约大量时间和经费的目的。根据国外对三种不同类型的“爱国

者”、“罗兰特”及“尾刺”地空导弹研制过程中的情况统计分析,可得到如下结论:由于采用虚拟及仿真技术,使靶试实弹数减少了 30%~60%;研制费用节省了 10%~40%;研制周期缩短了 30%~40%,其经济效益颇高。

美国陆军利用虚拟试验验证系统对“长弓海尔发”导弹进行小批量生产和大批量生成的验收试验,明显减少了传统的飞行试验次数,提高了导弹批次验收试验的可信度。据保守估计,使用上述验收设施的虚拟试验比实际试验每年至少节省 500 万美元,最高能达到 1000 万美元。美军完成 M1 改进型主战坦克的作战试验,采用实物模拟,需要花费两年时间,耗资 4000 万美元;而采用虚拟试验,则只需 3 个月时间,耗资近 640 万美元,其效果显而易见。

2. 可靠性仿真试验的内涵和发展趋势

随着信息技术、建模与仿真、虚拟现实、人工智能、计算机网络等技术的飞速发展,以及仿真、虚拟技术与试验评价技术融合,仿真试验技术应运而生。将仿真试验技术应用到可靠性领域,形成基于仿真试验的可靠性验证评价技术,即可靠性仿真试验与评价技术,是目前可靠性试验技术的研究热点和发展趋势之一。

(1) 仿真试验的内涵

仿真试验又称虚拟试验,仿真试验是在长期积累的大量有关数据、动力学模型以及各类三维模型的基础上,利用高性能计算机、网络环境、传感器或各种虚拟现实设备,建立能方便地进行人机交互的虚拟环境或虚拟与实际结合的环境,在此环境中对实体、物理样机或虚拟样机进行试验,用可视化的方法观察被视物体的性能及其相互间的关系,并对试验结果进行分析与研究。例如:虚拟风洞、发动机试车仿真试验、飞行仿真试验等。

从广义上讲,任何不使用或部分使用实际硬件来构造试验环境,完成实际物理试验的方法和技术都可以称为仿真试验。

仿真试验技术的作用主要体现在它搭建起产品数字化设计和性能试验的桥梁,通过构建数字化的试验和测试环境,利用计算机技术、信息处理技术、CAX (CAD/CAE/CAPP/CAM) 技术、虚拟现实等技术,对指定试验的特殊属性进行数字化检测,为设计人员提供产品功能、性能等多方面的信息,使设计人员能够根据设计方案方便、快捷地评估产品的各项性能与可靠性等指标。从虚拟试验的内容方面看,仿真试验往往对照传统实物试验的试验目的进行,对已经能够利用数学模型描述的部分进行仿真建模,得到虚拟试验样机,在此基础上进行仿真预示,开展相关的试验验证活动。顾名思义,仿真技术是仿真试验不可或缺的关键技术和有效手段。

仿真试验意味着试验手段、对象和环境应力等都是虚拟的。仿真试验技术属于



可控制的、无破坏性的、耗费小并允许多次重复的试验手段。在复杂产品的研制过程中, 仿真试验不仅可以作为真实试验的前期准备工作, 而且可以在一定程度上替代传统的物理试验, 减少物理样机制造试验次数, 使试验不受场地、时间和次数的限制, 并实现对试验过程的记录、重复与再现, 实现设计者、产品用户在设计阶段信息的互反馈, 使设计者尽早发现并解决设计过程中存在的潜在问题, 从而达到缩短新产品试验周期、降低试验费用、提高产品质量的目的。

但是, 仿真试验并不能完全代替真实试验, 二者具有互补性。真实试验除了可以为仿真试验模型的确认提供必要的数据和信息外, 还可以发现仿真试验不能涵盖的问题。

(2) 可靠性仿真试验

① 目的。

在产品研制的早期, 发现设计上的可靠性薄弱环节并指明原因, 指导设计改进, 提高产品固有可靠性, 以及对产品可靠性水平进行预先评估。

② 适用阶段。

开始于产品详细设计阶段, 随着研制进度的循环迭代, 直至产品设计定型前最终完成。

③ 主要特点。

可靠性仿真的特点主要包括:

- 是一种基于物理故障的可靠性技术, 采用建模与仿真手段, 对产品的可靠性进行分析和评估的工程方法。
- 与性能设计并行开展, 及时地支撑设计人员进行可靠性设计和优化。
- 采用数字样机与计算机仿真, 不受物理样机和试验资源限制。
- “建模仿真—物理试验—模型修正”是可靠性仿真试验最有效的运行方式。

④ 原理和主要流程。

可靠性仿真试验的原理图如图 1-14 所示, 主要原理和流程如下。

- 输入(导入)产品的数据化样机, 寿命周期环境条件, 使用条件, 设计信息等。
- 按照产品的使用(任务)剖面仿真输入热、电、振动、机械等方面的应力(可应用 FLOTERM、ANSYS 等)。
- 应用失效物理模型库和相应的仿真软件工具(如美国马里兰大学的 Calce PWA、工业和信息化部电子第五研究所的 pofRAS 等), 进行故障模式/机理及影响分析(FMMEA)、累积损伤分析和蒙特卡洛仿真等手段, 预测产品的平均首次故障时间, 找出相应主故障机理。

- 根据上述故障预计，综合运用故障分布拟合、故障聚类、多分布综合和可靠性综合评估等手段，评估产品的可靠性水平。
- 输出仿真试验结果，主要包括产品的可靠性薄弱环节及建议的改进措施，可靠性综合评估结果等。

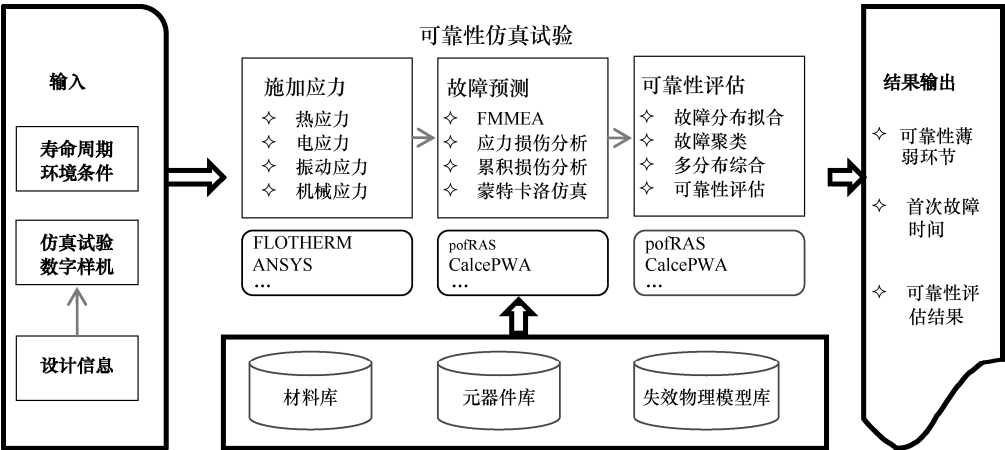


图 1-14 可靠性仿真试验原理示意图

由国内外型号产品项目中的应用实践表明，可靠性仿真试验可以有效克服实物试验的局限性，显著缩短研制周期、降低技术和项目风险，以及研制成本，已成为与可靠性实物试验并举（或作为必要补充）的一种新的试验形式。可靠性仿真试验与实物试验可以相辅相成，互为补充。可靠性仿真试验可以弥补实物试验的不足，尤其是对子样或试验过程中会对试验对象严重损伤的情况下，但仿真试验的成功建立在大量实物试验积累的数据基础上，实物试验通过提供虚拟试验模型，以及仿真验证和确认时所需的信息来改进仿真试验的效能和精确度。

1.5.13 高加速极限试验和应力筛选

1. 高加速极限试验和应力筛选的起源

随着科学技术的发展，现代电子设备的复杂程度越来越高，发展也很快，可靠性问题也越来越尖锐，传统的可靠性环境模拟试验已经远远不能赶上现代电子设备发展的步伐。激发试验就是在克服环境模拟试验的试验周期长、试验效率低、试验耗费大等缺点的基础上发展起来的一种新的可靠性试验技术。

激发试验与环境模拟试验思路不同，它不是模拟真实环境，而是对试件施加比产品实际使用条件残酷得多的环境和工作应力，快速激发并排除产品潜在的缺陷来达到提高产品可靠性和缩短高质量产品研制周期的目的。激发试验可实现在不足原

来 1/5~1/10 试验费用的情况下，获得的可靠性水平是传统试验的数百倍。

美国 G. K. Hobbs、K. A. Gray 和 L. W. Condra 等人最早开始从事研究如何采用强化应力激发缺陷的方法，快速有效地暴露设计薄弱环节和剔除制造工艺缺陷的试验技术，并把他们所研究的试验方法称为高加速极限试验（Highly Accelerated Limited Test，HALT）和高加速应力筛选（Highly Accelerated Stress Screen，HASS），前者是针对设计的，后者是针对生产过程的。这种方法的核心是对产品施加大大超过设计规范的极限应力，一步一步地添加，逐渐排除缺陷，故又称为步进应力试验方法。

值得注意的是，HALT 以往被作为高加速寿命试验的简写，这样的简写容易造成混淆。HALT 作为非指标考核性的加速试验，不能得到产品的寿命信息，但可以得到产品设计应力极限值的信息，因此称为高加速寿命试验是不合适的。

以往，环境试验被作为一种产品预期要经受外场实际环境的模拟试验。研制产品时通常把技术条件规定的应力极限值作为鉴定或考核产品的条件，但是，即使已顺利通过了设计阶段的鉴定试验和生产阶段的验收试验，残留的潜在缺陷仍然很多，大量产品使用时可靠性差，平均故障间隔时间（MTBF）短，外场返修频繁，导致担保费用、维修费用居高不下，用户或客户不满意，严重影响研制部门和制造厂商的信誉。

传统的可靠性试验，包括环境应力筛选（ESS）、可靠性增长试验和可靠性鉴定试验等，大多是在模拟环境下进行的试验，以 ESS 为例，最早电子产品的 ESS 是根据美国海军 1979 年 NAVMAT-P9492《生产筛选试验大纲》确定的。温度范围一般采用技术条件规定的上下限，温度循环次数由产品的复杂程度决定，如表 1-1 所示。

表 1-1 温度循环次数与产品的复杂程度

产品元器件数量	<100	100~500	500~1000	1000~2000	2000~4000
循环次数	2	4	6	8	12

可靠性增长试验则选用模拟现场实际的综合环境条件进行。GJB 1407-92《可靠性增长试验》规定可靠性增长的总试验时间一般为（5~25）MTBF。这些试验费用昂贵，试验时间长，而价格和研制周期已成为当今市场激烈竞争的焦点，因此研究开发一种快速、经济、有效的新的可靠性试验方法已势在必行。HALT/HASS 就是在这种背景下产生的。

- HALT 是一种试验方法（思想），采用的环境应力比加速试验更加严酷，主要应用于产品开发阶段，它能以较短的时间促使产品的设计和工艺缺陷暴露出来，从而为设计改进，提升产品可靠性提供依据。

- HASS 是产品通过 HALT 试验得出工作或破坏极限值后在生产线上做高加速应力筛选，要求 100%的产品参加筛选。其目的是为了使得生产的产品不存在任何隐含的缺陷或至少在产品出厂前找到并解决这些缺陷。HASS 是通过加速应力方式以期在短时间内找到有缺陷的产品，缩短纠正措施的周期，并找到具有同样问题的产品。

HALT 和 HASS 作为一种激发试验方法，其理论依据是故障物理学。它把故障或失效当成研究的主要对象，通过激发、研究和根治产品缺陷达到提高可靠性的目的。

G. K. Hobbs 曾设计了一种试件，就强化应力对疲劳寿命的影响效果进行了研究，发现当应力强度增加 1 倍时，疲劳寿命降低为原来的 1/1000。对于有缺陷的产品，缺陷处应力集中系数高达 2~3 倍，疲劳寿命就相应降低好几个数量级，使得有缺陷元件和无缺陷元件在相同的强化应力作用下疲劳寿命拉大了档次，使有缺陷元件迅速暴露的同时无缺陷部件损伤甚小。这一试验结果也清楚地说明了 HALT/HASS 试验技术的基本原理。

表 1-2 给出了 G. K. Hobbs 博士的试验结果比较。

表 1-2 不同温变率的试验结果比较

变温率（℃/min）	5	10	15	18	20	25	30	40
循环次数	400	55	17	10	7	4	2.2	1
Min（次）	66	33	22	22	18.3	16.5	13.2	8
筛选时间（h）	440	30	6	3.0	3.0	1.9	0.9	0.1

2. HALT 和 HASS 的主要特点

HALT 是一种发现缺陷的工序，它通过设置逐级递增的、加严的环境应力来加速暴露试验样品的缺陷和薄弱点，而后对暴露的缺陷和故障从设计、工艺和用料等诸多方面进行分析和改进，从而达到提升可靠性的目的，最大的特点是设置高于样品设计运行极限的环境应力，从而使暴露故障的时间大大短于正常可靠性应力条件下的所需时间。环境应力筛选目的是利用环境应力使电子硬件在制造过程中较弱的零部件，以及由不良工序等因素造成的非设计问题尽可能早地暴露出来，进而可以采取修改行动或将之剔除，以提高产品质量，使之满足设计要求。

高加速应力筛选（HASS）是用显著高于预期使用或运输时的应力来对生产单元进行筛选，但应力水平比能够显著降低产品外场寿命的应力水平还要低，可基于高加速极限试验的结果确定。筛选的目的是为了发现产品在正常使用过程中可能出现的潜在缺陷。发现潜在缺陷后，应进行失效分析，并采取必要的纠正措施（通过

专门设计的检测特定失效模式的试验进行验证), 以降低故障的数量。其目的是在产品还没有出厂前找到并消除产品的隐含缺陷。HASS 就是通过加速应力方式以期在短时间内找到有缺陷的产品, 缩短纠正措施的周期。

HALT 的主要特点如下:

- HALT 试验施加的环境应力是以递增的形式变化的, 其试验过程是通过施加不断加大的应力来激发设计中潜伏的各种缺陷, 直到产品的破坏极限。
- HALT 试验在超出规范极限以外进行, 具有很高的试验效率。
- 在 HALT 过程中出现的失效模式是在远远超过设计规格的环境应力下激发出来的, 但这些失效模式都是在实际现场使用中所出现的失效形式, 否则 HALT 试验是无效的。
- HALT 试验的主要目的是查明和排除设计的薄弱环节, 评价产品设计的可靠性。

HALT 及 HASS 的主要优点如下:

- 为改进可靠性而选择性地增加并验证设计余量。
- 确定特定失效模式的样品量少。
- 可迅速确定特定应激源及组合应力的主要失效模式。
- 可高效地权衡数据分析和确定必要的纠正措施。
- 快速验证纠正措施。
- 高效的生产筛选。
- 从总体中消除薄弱或有缺陷的组件 (质量及可靠性改进)。

HALT 及 HASS 的主要不足包括:

- 激发的失效模式一般不能在产品使用过程中观测到。
- 有对设计余量过度改进的潜在可能 (过设计)。
- 不能得知试验后的可靠性。
- 试验结果的统计置信度有限 (过高或过低估计设计余量)。
- 测试结果未涉及多种失效模式的耦合作用。
- 对于较大、较小以及具有多种脆弱性的产品不适用。
- 应力种类 (主要是温度、振动及温度循环) 数量有限。
- 不能评估受其他应力类型 (除了 HALT 试验应力类型之外) 协同作用下的产品设计极限。

3. 发展现状和面临的挑战

从 20 世纪 80 年代末到 90 年代初, 国外很多国家 (特别是美国) 在各工业部

门开始推广、应用高加速应力试验（包括极限应力试验）技术，目前该技术已被广泛地应用于通信、电子、电脑、医疗、能源、航空、航天和军事等领域，涉及的产品有网络设备、微波设备、光纤、遥测设备、视频处理设备、商用航空电子、掌上电脑、半导体制造设备等，呈现出蓬勃发展的趋势。首先，国外许多为机械、电子工业提供设计、制造和试验服务的公司，已经把高加速应力试验（包括极限应力试验）作为一项很重要的服务内容，如为航空航天、军事工业和一般民用工业提供试验服务的美国 Garwood laboratories 公司，它所提供的一项重要服务就是产品的可靠性试验，其主要内容是高加速应力试验。在国外，HALT 和 HASS（High Accelerated Stress Screening）已成为军用和民用公司研发新产品的重要手段，很多为机械、动力、化工提供设计、制造和试验服务的公司，已经把 HALT 作为一项重要的服务内容。比如美国的 Garwood Laboratories 公司，把 HALT 作为提高产品质量、降低产品保证期召回率的一项重要技术手段，所服务的客户包括雷神飞机、波音、索尼等著名公司。提供机械工程方面技术支持的公司如美国 Dalse Engineering Solutions 公司、美国电子加工服务供应商 MCMS 公司、美国的 Wyle Laboratories 公司、美国的 Telephonic 公司等把 HALT 作为一种重要的质量保障服务提供给用户，并广泛赢得了各工业部门的客户。据报道，美国 Dalse Engineering Solutions 公司曾依靠 HALT 技术来帮助改进有关工业设备产品质量和加工能力，使其销售额提高了 35%。

国内对 HALT 和 HASS 的探索刚刚起步，工业和信息化部电子五所、国防科技大学可靠性实验室和北京航空航天大学可靠性工程中心等有部分军工型号中取得初步应用成效；一些大型通信公司，如华为、中兴已经开始重视 HALT 和 HASS 技术的应用并取得了一定成效；在航天、航空等领域也开展了工程实践，例如，20 世纪末曾对液体火箭发动机和惯性仪表进行了 HALT 实验。

虽然我国在 HALT 及 HASS 的研究、应用方面取得了一定成效，但对其核心技术的掌握不全面，有待进一步深入研究实践。目前，HALT 和 HASS 领域主要存在的问题和挑战有：

- 高加速应力下的失效机理和规律。
- 加速环境选择与试验剖面确定技术。
- 应力加载与试验技术。
- 试验结果分析和评估技术。
- 缺乏相应技术标准和规范。
- 相关的试验设备、夹具设计、安装方式、信号监测、采集技术以及控制技术。
- 计算机辅助 HALT 和 HASS 仿真技术。



参 考 文 献

- [1] GB/T 19000-2008/ISO 9000:2005. 质量管理体系基础和术语.
- [2] IEC 60500-192:2015 INTERNATIONAL ELECTROTECHNICAL VOCABULARY-Part 192: Dependability.
- [3] GJB 451A-2005. 可靠性维修性保障性术语.
- [4] 曾天翔, 等. 可靠性及维修性工程手册. 北京: 国防工业出版社, 1994.
- [5] 黄进永, 冯燕宽, 张三娣. 复杂系统理论在复杂网络系统可靠性分析上的应用. 质量与可靠性, 2009, 23~27.
- [6] 张红林. 动态系统可靠性分析关键技术. 国防科学技术大学工学博士学位论文, 2011.
- [7] 江式伟, 等. 基于时间 Petri 网的装备体系可靠性建模与仿真. 系统工程与电子技术, 2013, 35 (4): 896~899.
- [8] 涂刚, 郭基联. 基于作战任务的航空装备体系可靠性分析. 军事运筹与系统工程, 2014, 28 (3): 53~56.
- [9] 王中杰, 谢璐璐. 信息物理融合系统研究综述. 自动化学, 2011, 37 (10): 1157~1166.
- [10] Pan Yong, Hu Ning. Research on Dependability of Cloud Computing Systems, Proceedings of the 10th International Conference on Reliability, Maintainability and Safety, 2014.
- [11] 陈冰泉. 云计算服务系统可靠性建模研究. 电子产品可靠性与环境试验, 2014, 32 (2): 22~28.
- [12] Yang B, Tan F, Dai YS, Guo S. Performance evaluation of cloud service considering fault recovery. In Proceedings of the first international conference on cloud computing (CloudCom 2009). Lecture notes in computer science, 2009, 5931: 571~576.
- [13] <http://www.cloudbus.org/cloudsim/>.
- [14] 彭建. 基于失效物理的电子系统的可靠性预计研究与实现. 电子科技大学硕士学位论文, 2012.
- [15] 张宝珍. 国外综合诊断、预测与健康管理技术的发展及应用. 计算机测量与控制, 2007, 591~594.
- [16] 于晓伟, 张宝珍. 国外电子产品故障预测技术的发展. 测控技术, 2008.
- [17] 曾声奎, Micheal G.Pecht, 等. 故障预测与健康管理 (PHM) 技术的现状与发展. 航空学报, 2005, 26 (5): 626~632.

- [18] 肖刚, 李天柁, 余梅. 动态系统可靠性仿真的五种蒙特卡罗方法. 计算物理, 2001, 18 (2): 173~175.
- [19] 金光. 动态系统可靠性建模与高可靠度系统仿真研究. 国防科学技术大学博士学位论文, 2000.
- [20] 金光. 动态系统可靠性分析的新概念. 国防科技大学学报, 2004, 26 (2): 100~105.
- [21] 沈戈, 苏春, 许映秋. 基于 Petri 网理论的动态系统可靠性建模方法研究. 机械工程与自动化, 2006, (2): 1~9.
- [22] 康锐, 王自力. 装备全系统全特性全过程质量管理概述. 国防技术基础, 4: 25~29.
- [23] 熊刚强. 装备通用质量特性的学习与对策探讨. 化工管理, 2014, 10: 74~77.
- [24] 吴明福. 通用质量控制系统的研究. 东北大学硕士学位论文, 2008.
- [25] 邵家骏. 大型软硬件综合系统的质量与可靠性管理. 质量学术专刊, 2002, 12: 41~45.
- [26] 何大韧, 刘宗华, 汪秉宏. 复杂网络的一些统计物理学方法及其背景. 力学进展, 2008, 38(6): 692~701.
- [27] 马致考. 重正化群方法及应用. 西北大学学报, 1998, 28 (1): 30~33.
- [28] 肖柳青. 复杂网络统计系统理论及其应用研究. 上海交大博士学位论文, 2009.
- [29] 邓小龙, 王柏, 吴斌, 杨胜琦. 基于信息熵的复杂网络社团划分建模和验证. 计算机研究与发展, 2012, 49 (4): 725~734.
- [30] 韦金昌. 复杂生态系统的广义信息熵理论及应用. 天津大学硕士学位论文, 2009.
- [31] 李德毅, 刘常昱. 论正态云模型的普适性. 中国工程科学, 2004, 6 (8): 30~32.
- [32] 贾小平. 军用电子模块无铅焊点可靠性的研究. 清华大学工程硕士专业学位论文, 2011.
- [33] 史耀武. 无铅替代及对电子组装可靠性的影响. 电焊机, 2009, 39 (1): 5~11.
- [34] 顾永莲, 杨邦朝. 无铅焊点的可靠性问题. 电子与封装, 2005, 5 (5): 12~16.
- [35] Way Kuo. 纳米电子时代可靠性研究的挑战. 质量与可靠性, 2006, (6): 53~59.
- [36] 袁博. 纳米电子系统的容缺陷设计方法研究. 中国科学技术大学博士学位论文, 2014.
- [37] 张宝珍. 虚拟试验与仿真验证技术在国外武器装备研制中的应用. <http://www.cetin.net.cn/qrms/>.
- [38] 胡叶楠, 陈海东, 等. 虚拟试验技术体系及其应用研究初探. System Simulation Technology & Application, 2011 (13): 527~532.
- [39] 姜同敏. 可靠性与寿命试验. 北京: 国防工业出版社, 2012.



- [40] 杨春虹, 李斌, 等. 高加速应力试验及极限应力试验综述. 电子与封装, 2006, 42 (10): 31~38.
- [41] IEC 62506: 2013 Methods for product accelerated testing.
- [42] 赵婉. HALT 技术在我国航天产品中的应用前景分析. 质量与可靠性, 2010, 149 (5): 46~48.

第2章

可靠性基础

2.1 对可靠性定义的进一步理解

2.1.1 可靠性的构成要素

在第1章，我们已经给出了可靠性的定义。如前所述，可靠性是指产品在规定的条件下和规定的时间内，完成规定功能的能力，其概率称为可靠度。

产品可靠性定义包括下列4个要素：

- 规定的环境和使用条件。
- 规定的任务和功能。
- 规定的时间。
- 规定的能力。

在4个要素中，前3个描述前提条件，第4个描述判定依据：是否具备这样的能力。对于一个具体的产品，应按上述要素分别给予具体明确的定义。

图2-1列出了产品可靠性的4个要素及其简要说明。

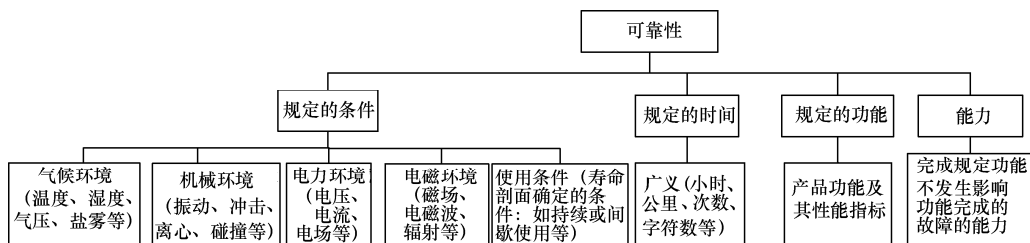


图 2-1 可靠性的要素

2.1.2 规定的任务和功能

规定的功能是指产品功能及其性能指标，例如通信设备的信号发送和接收功能。

产品能否完成预定的任务，取决于其各种功能是否正常。对于具有单一功能的简单产品，其无故障工作的定义比较容易；而对于具有多种功能的复杂产品，其无故障工作的定义必须进行细致的分析才能做出，比如一台电视机，完成任务就是对一定的电视信号，能播放出良好的伴音和图像来；而对伴音和图像这两种功能及其保证又涉及其主要技术指标的满足和完成上述功能有关组件的正常工作。根据对各组件的故障模式和影响的分析，可进一步规定各组件的性能指标的可接受范围、各组件正常工作的条件，最后给出无故障工作的具体定义。同样，根据不可接受的指标范围而给出故障的定义。

2.1.3 规定的环境和使用条件

规定的条件，包括两层意思：

- 一是产品使用场所的环境条件。产品的环境条件主要是指执行任务所遇到的环境条件，但同时必须注意到运输、储存以及工艺过程中引入的环境影响。环境条件主要包括气候环境（温度、湿度等）、机械环境（如振动、冲击等）、电应力环境（如电压、电流等）、电磁环境（磁场、电磁波等）等。
- 二是产品的使用条件，即产品的使用状态，与“寿命剖面”确定的条件相关。例如，产品是持续工作的还是间歇工作的。飞机执行一次任务经历滑行、起飞、巡航、降落等阶段，在这些不同的阶段，飞机遭遇的环境和使用条件是不一样的。

环境可按照一定的使用场合进行分类，如地面条件良好、一般地面固定、恶劣地面固定、空间轨道飞行、车载、舰船、飞机等。GJB/Z 299C《电子设备可靠性预计手册》给出了电子设备典型的使用环境类别及其详细说明，如表 2-1 所示。

在可靠性技术中，必须强调环境的影响，因为同样的产品在不同的温度和环境条件下运行时，其可靠性是不同的。恶劣环境下的失效率可能会达到良好环境下的 30~50 倍。在确定产品的可靠性要求时，应明确产品使用的环境条件，以便在设计时进行这方面的考虑。

产品在规定的条件下使用是可靠性定义的前提条件，一旦超越了规定的条件，则产品极有可能损坏或故障，但这种情况与产品的可靠性无关。举一个简单的例

子，把规定在室内使用的显示器放置在室外使用，由于没有防水功能，一旦下雨，使用时必然发生故障，无法工作，但不能因此说这个显示器的可靠性差，因为它发生故障的原因是不按规定的条件使用。同理，把一个额定电压为 110V 的电器接到 220V 的电源插座，也必然会烧坏。这也不是该电器的可靠性问题，而是由于不按规定的条件使用所致。

表 2-1 GJB/Z 299C 的环境类别说明

环境类别	符号	说 明
地面良好	G _B	能保持正常气候条件，机械应力接近于零的地面良好环境，其维护条件良好，例如有温湿度控制的实验室或大型地面站等
导弹发射井	G _{MS}	发射井中的导弹及其辅助设备所处的环境
一般地面固定	G _{F1}	在普通的建筑物内或通风较好的固定机架上，受振动、冲击影响很小的环境条件，如固定雷达、通信设备、电视机、收录机等家用电器所处的环境
恶劣地面固定	G _{F2}	只有简陋气候防护设施的地面环境或地下坑道，其环境条件较恶劣，如高温、低温、温差变化大、高湿、霉菌、盐雾和化学气体等
平稳地面移动	G _{M1}	在比较平稳的移动状态下，有所振动与冲击，例如在公路上行驶的专用车辆及火车车厢环境
剧烈地面移动	G _{M2}	安装在履带车辆上，在较剧烈的移动状态下工作，受振动、冲击影响较大，通风及温湿度控制条件受限制，使用中维修条件差，例如装甲车内的环境条件
背负	M _P	由人携带的越野环境，维护条件差
潜艇	N _{SB}	潜艇内的环境条件
舰船良好舱内	N _{S1}	行驶时较为平稳，且受盐雾、水汽影响较小的舰船舱内，如近海大型运输船和内河船只的空调舱
舰船普通舱内	N _{S2}	能防风雨的普通舰船舱内，常有较强烈的振动和冲击，如水面战船舱内或甲板以下的环境
舰船舱外	N _U	舰船甲板上的典型环境，经常有强烈的冲击和振动，包括无防护、暴露于风雨下的环境
战斗机座舱	A _{IF}	战斗机飞行员座舱环境，无太高的温度、压力和过于强烈的冲击振动
战斗机无人舱	A _{UF}	有高温、高压、强烈的冲击与振动等恶劣环境条件，如战斗机机身、机尾、机翼等部位的设备舱、炸弹舱
运输机座舱	A _{IC}	运输机空勤人员的座舱环境
运输机无人舱	A _{UC}	运输机上无环境条件控制的非载人区域环境
直升机	A _{RW}	在带旋转翼直升机机内或机外安装的环境
宇宙飞行	S _F	在地球轨道上飞行，不包括动力飞行和重返大气层，例如卫星中电子设备的安装环境
导弹发射	M _L	由于导弹发射、火箭飞行、射入轨道、重返大气层或降落伞着陆等引起的噪声、振动、冲击以及其他恶劣的环境条件
导弹飞行	M _F	与吸气助燃推进导弹、巡航导弹的动力飞行和处于无动力自由飞行导弹相关的环境条件

2.1.4 规定的时间

可靠性是与时间密切相关的产品属性。这里的时间是指广义的时间概念，可以

是日历时间、使用时间，也可以是使用次数、里程、循环数等寿命单位。产品的可靠性一般随着时间的推移呈下降趋势。

注意，产品在规定的时间内可能存在多种状态，即工作、部分工作或非工作状态，因此，考虑产品的可靠性时，应把产品的各种状态的持续时间及其对应的环境联系起来。

例如，一台电视机可能存在完全工作（正常开机）、部分工作（如待机、伴音模式）和非工作（关机，完全切断电源）3 种状态，在这些不同的状态下，系统各组成部分的工作状况是不同的。在计算其可靠性参数时，必须将其各种工作状态及其持续时间和环境（如待机状态下的环境温度会比工作状态下的低得多）联系起来。

为了更好地理解与可靠性相关的时间概念，我们用图示方式说明时间的分解，见图 2-2。

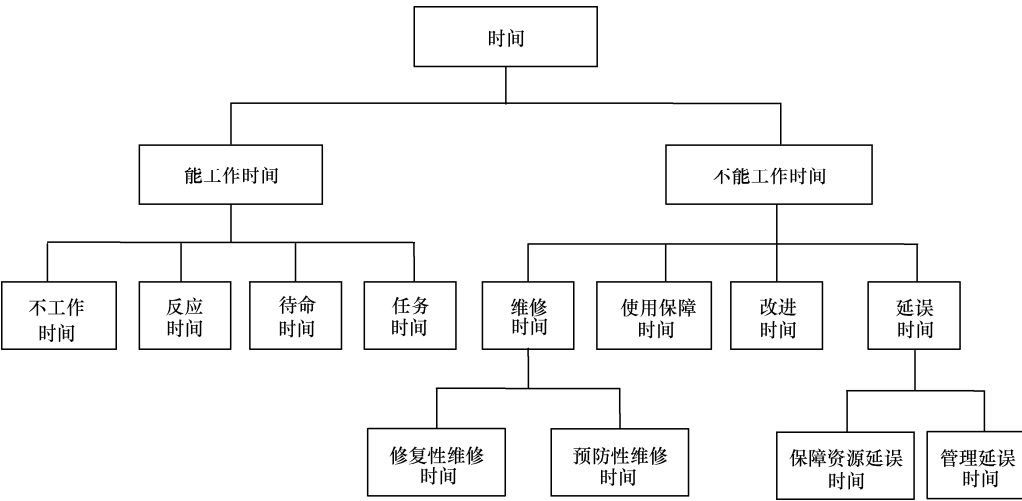


图 2-2 时间图解

对相关的时间概念说明如下：

- 能工作时间（up time）：产品处于执行其规定功能状态的时间。
- 不能工作时间（down time）：产品不处于执行其规定功能状态的时间。
- 不工作时间（not operating time）：产品能工作，但不要求其工作的时间。
- 反应时间（reaction time）：产品从要求执行某项任务的瞬间开始到准备好执行该任务所需的时间。它是产品从不工作状态转入工作状态所需的时间。
- 待命时间（alert time）：产品从准备好随时可执行其任务到开始执行任务的等待时间。在这段时间内，不进行维修或妨碍任务开始的其他活动。

- 任务时间 (mission time): 产品执行某项规定任务剖面所用的能工作时间。
- 使用保障时间 (operational support time): 为产品的使用提供保障, 以确保其完成规定的任务所用的时间, 如民用客机出动前的补充水和食物、加油时间等。
- 维修时间 (maintenance time): 停机维修所用的时间, 不包括改进时间和延误时间。
- 预防性维修时间 (preventive maintenance time): 产品进行预防性维修所用的时间。
- 修复性维修时间 (corrective maintenance time): 对产品进行修复性维修所用的时间。
- 改进时间 (modification time): 为改善产品特性或增加新的特性而对其进行更改所用的时间。
- 延误时间 (delay time): 由于保障资源补给或管理原因未能及时对产品进行保障所延误的时间。
- 保障资源延误时间 (logistic delay time): 因等待所需的保障资源而未能及时对产品进行保障所延误的时间, 如等待备件、维修人员、保障设备、信息及适当的环境条件等所延误的时间。
- 管理延误时间 (administrative delay time): 由于管理方面的原因而未能及时对产品进行保障所延误的时间。

2.1.5 规定的能力

能力的表征方式有定性和定量两方面: 定性方面主要是产品是否具备相应的能力, 定量方面一般用比值描述其完成规定功能的概率, 即可靠度。

产品的可靠度与故障发生的频度密切相关。为此, 我们必须首先明确故障和失效的概念。

1. 产品失效的概念

在开展可靠性工作过程中, 经常会把故障、失效、缺陷这些概念混淆。

在 GJB 451A《可靠性维修性保障性术语》中给出了故障、失效的定义。

- 故障 (fault/failure): 产品不能执行规定功能的状态。通常是指功能故障。因预防性维修或其他计划性活动或缺乏外部资源造成不能执行规定功能的情况除外。
- 失效 (failure): 产品丧失完成规定功能的事件。在实际应用中, 特别是对

硬件产品而言，故障与失效很难区分，故一般统称为故障。

可以这么理解，故障与失效的区别在于失效描述的是事件，故障描述的是状态，故障是由失效产生的状态。失效了必然有故障，有故障不一定就已经失效。有时候失效前已产生了一定的故障。工程中有带病运行的情况，这时候故障已经出现且在不断发展中，但尚未失效。

而缺陷（flaw）是指可导致产品失效或故障的缺点。产品的缺陷在设计或制造过程中产生，这些缺陷一旦在使用中被激活，则会引发产品失效或故障。

2. 产品失效的分类

产品失效可以按多种方式分类，如按失效原因、程度、可否预测、发生速度、危害程度、特征，以及产品寿命周期等分类，常见的失效分类如表 2-2 所示。

表 2-2 失效的分类及定义

分类原则	失效名称	定 义	举 例
按失效原因	误用失效	不按规定的条件使用产品而引起的失效	使用非合适型号的汽油，导致发动机损坏
	本质失效	按规定的条件使用产品，由产品固有的弱点引起的失效	中华骏捷 FSV 刹车失灵或发动机长期使用，导致气门封闭不严
	独立失效	不是由其他产品失效引起的失效	轮胎爆裂
	从属失效	由其他产品失效引起的失效	冷却系统故障，导致暖气系统无法正常工作
按失效程度	完全失效	产品的性能超过某种界限，以致完全丧失规定功能的失效	发动机太热，发动机零件损坏，无法启动
	部分失效	产品的性能超过某种界限，但没有完全丧失规定功能的失效	部分零件使用失效，冷却液泄漏，发动机冷却功能减弱
按失效可否预测	突然失效	通过事前检测或监控不能预测到的失效	突发车祸，刹车失灵
	渐变失效	通过事前或监控可以检测到的失效	轮胎磨损，刹车片磨损严重
按失效发生速度	突变失效	部分发生完全失效	刹车液压油管堵塞，刹车失灵
	退化失效	渐变而部分发生失效	油门长期使用，松懈，加油不给力
	间歇失效	产品失效后，不经修复而在限定的时间里，能自行恢复功能的失效	冬天发动机不易启动，天气暖和后自行改善
按失效危害程度	致命失效	可能导致人或物重大损失的失效	突发车祸，车辆变形严重
	严重失效	可能导致复杂产品降低完成规定功能能力的产品组成单元的失效	活塞磨损漏气，发动机动力不足
	轻度失效	不致引起复杂产品降低完成规定功能能力的产品组成单元的失效	滤清器损坏，供油系统故障，发动机无法正常工作

(续表)

分类原则	失效名称	定 义	举 例
按失效特征	相关失效	在解释使用结果或计算可靠性特征量的数值时，必须计入的失效	活塞裙部半径加上环形防漏气的垫圈
	无关失效	在解释使用结果或计算可靠性特征量的数值时，不应计入的失效	汽车总重量不计入人的质量
按产品工作期	早期失效	因设计、制造、材料等方面的缺陷，使产品在工作初期发生的失效	导航系统无法更新，道路发生改变，无法正常导航
	偶然失效	产品在使用中，由偶然因素发生的失效	车内失火，座椅损坏，无法正常驾驶
	耗损失效	由于老化、磨损、耗损、疲劳等原因，使产品发生的失效	轮胎磨损失效，车灯损坏，蓄电池充不进去电

3. 产品失效的规律

统计数据和工程经验表明，产品的失效一般有一定的规律可循。

产品失效的概率称为失效率，产品的瞬时失效率是时间的函数。一般来说，产品的失效率曲线有递增型、递减型以及常数型等。在长期的可靠性实践中，人们发现许多产品都服从一条典型的失效率曲线。这条曲线与人的死亡率曲线相似，具有两头高、中间低的特点，形状很像一个洗浴用的盆，因此，人们习惯性地称之为“浴盆曲线”，如图 2-3 所示。

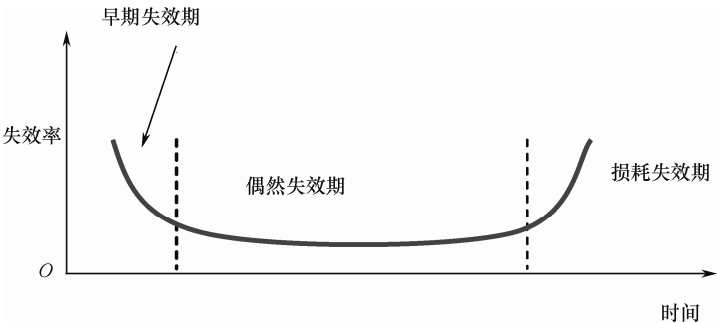


图 2-3 浴盆曲线

从这条曲线可以看出，产品的失效有 3 个阶段，早期失效期、偶然失效期和耗损失效期。早期失效期的特点是开始时失效率高，后来逐渐降低。在产品设计过程中，为了缩短早期失效期的时间，在产品投入运行、使用前，一般都要进行试运行或者通过试验进行筛选，剔除不合格产品。偶然失效期的特点是产品失效率低而稳定，可近似地看成一个常数。耗损失效期的特点是产品的失效率随工作时间的增长而上升。

应当看到，通常我们讲的指数分布可近似地认为是浴盆曲线的底部，即偶然失

效期。另外，有些产品没有损耗期，例如软件产品就没有损耗期，除非硬件耗损，质量高的半导体器件，其磨损期也是很明显的。

大多数电子产品的失效率曲线具有典型性，呈现两头高、中间低且平直的特性，一般服从指数分布，见第 2.3.1 节。

在指数分布的情况下，可以证明，产品的失效率是一个常数。这个结论也为多年的可靠性工程实践所证实。许多电子产品经过筛选后，都处于偶然失效期，其失效可以近似为常数，其分布特征可采用指数分布来描述。

2.2 产品的可靠性参数

2.2.1 常用的可靠性参数

1. 可靠度

产品在规定的条件下和规定的时间内，完成规定功能的概率称为产品的可靠度。若以 T 表示产品的寿命，以 t 表示规定的时间，显然，“ $T > t$ ”的事件是一个随机事件。产品的可靠性是用概率来度量的，因此，产品可靠度的数学表达式为：

$$R(t) = P(T > t) \quad (2-1)$$

式中， T 为产品寿命， t 为规定时间。

显然，当 $t=0$ 时， $R(0)=1$ ；当 $t=\infty$ 时， $R(\infty)=0$ 。

$$R(t) = \frac{N_0 - r(t)}{N_0} \quad (2-2)$$

式中： N_0 —— $t=0$ 时，在规定条件下工作的产品数；

$r(t)$ —— 在 $0 \sim t$ 内，累计的故障数。

【例 2-1】可靠度的计算

有一批产品，从中抽取 15 个样品试验，失效情况见图 2-4。在该柱状图中，纵坐标表示样品编号，横坐标表示试验时间（h），每一样品的柱子长度表示该样品的寿命终结时间，则在 1000h 时，其可靠度的观测值为：

$$\overline{R(t)} = \frac{6}{15} = 0.40$$

产品的可靠性参数是一个统计量值，就可靠度而言，它同产品在一定时间内的合格率或翻修率有密切的关系，是产品 $t > 0$ （可理解为产品交付用户使用后）时产品质量的重要度量指标。

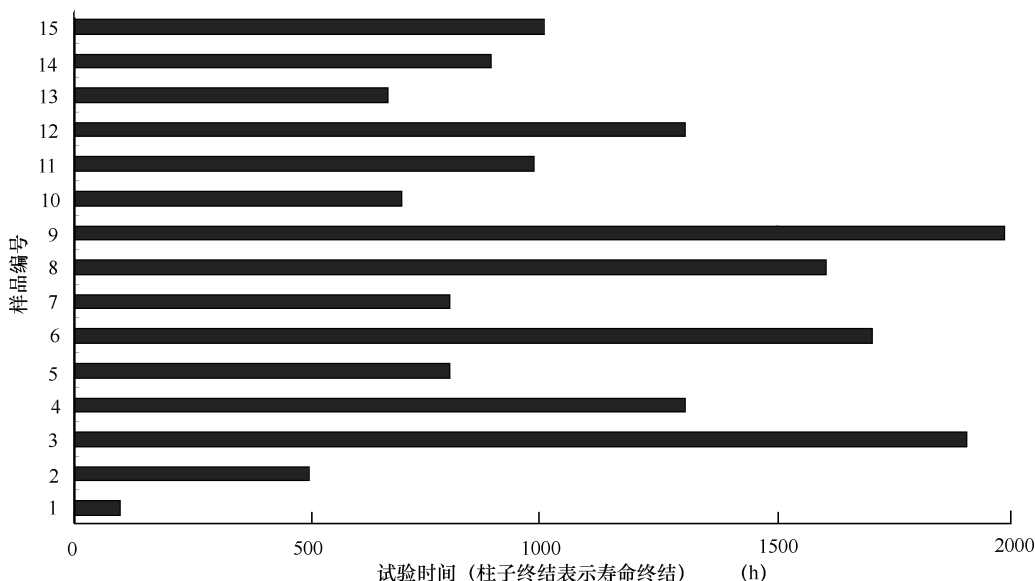


图 2-4 样品失效时间与可靠度计算

【例 2-2】规定条件可靠度的理解

某金属膜电阻在温度为 25°C 和流过电流 200mA 的条件下工作 1000 小时，其阻值变化不超过 $\pm 3\%$ 的概率为 99% ，则该电阻在这些规定的条件下的可靠度为 99% 。显然，当环境温度不同，电流负荷不同，工作时间不同，参数漂移要求不同时，电阻的可靠度也会不同。

【例 2-3】可靠度的理解

某种型号的洗衣机在普通家庭连续工作 4 年的可靠度是 95% ，如果用频率来解释概率，则意味着，这种洗衣机若售出 100 台，则 5 年内大约有 95 台不会发生故障， 5 台会发生故障。

2. 不可靠度

定义：是指产品在规定的条件下，在规定的时间内、产品不能完成规定功能的概率。它也是时间的函数，记作 $F(t)$ ，称为累积失效概率。产品的寿命是一个随机变量，对于给定的时间 t ，概率论中称随机变量 T 不超过规定值 t 的概率为分布函数，因此产品失效分布函数的数学表达式为：

$$F(t)=P(T\leq t) \quad (2-3)$$

显然，产品的可靠度与不可靠度之间，有关系式：

$$R(t)+F(t)=1$$

如【例 2-1】所示，其 1000 小时的不可靠度为 0.6 。



3. 失效概率密度函数

若函数 $F(t)$ 是连续可微的, 则其导数称为产品的失效概率密度函数。失效概率密度函数 $f(t)$ 表示产品在 t 时刻的单位时间内的失效概率。其数学表达式为:

$$f(t) = \frac{dF(t)}{dt} \quad (2-4)$$

显然, 产品的累积失效概率与失效概率密度函数之间有关系式:

$$F(t) = \int_0^t f(t) dt$$

因而, 产品的可靠度可表示为:

$$R(t) = 1 - F(t) = 1 - \int_0^t f(t) dt = \int_t^{\infty} f(t) dt \quad (2-5)$$

4. 失效率 (也称瞬时失效率)

在 t 时刻, 尚未失效的产品, 在该时刻后的单位时间内发生失效的概率, 称为产品的瞬时失效率, 简称为失效率。其数学表达式为:

$$\lambda(t) = \frac{f(t)}{R(t)} \quad (2-6)$$

由于 $f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt}$, 因而有:

$$\lambda(t) = -\frac{dR(t)}{dt} \cdot \frac{1}{R(t)} = -\frac{d \ln R(t)}{dt}$$

上述两边积分可得到:

$$-\int_0^t \lambda(t) dt = \ln R(t)$$

两边取指数得到:

$$R(t) = e^{-\int_0^t \lambda(t) dt}$$

由上式还可以得到:

$$f(t) = \lambda(t) e^{-\int_0^t \lambda(t) dt}$$

令 $\psi(t) = \int_0^t \lambda(t) dt$, 则称 $\psi(t)$ 为区间 $[0, t]$ 上的累积失效率。

令 $\bar{\lambda}(t) = \frac{\psi(t)}{t}$, 则称 $\bar{\lambda}(t)$ 为区间 $[0, t]$ 上的平均失效率。

某些产品的可靠性, 特别是电子元器件的可靠性, 常用失效比例来表示。

【例 2-4】平均失效率的理解

通俗地理解平均失效率，它可用公式表示如下：

平均失效率=失效产品的百分比/工作时间

例如，某种调谐器的平均失效率为 2%（每 1000 小时），意味着 100 只这种调谐器使用 1000 小时平均有 2 只失效。

① 失效率的单位。

通常可以采用每小时 1%或千小时的 1%来作为产品失效率的单位，但对可靠要求高的产品来说，就需要采用更小的单位来作为失效率的基准。现在常采用菲特作为基准单位。菲特这一单位的数量概念是：

1 菲特（FIT）=1×10⁻⁹/小时

实际上，这就表示了 10 亿个元件 1 个小时内只允许有一个产品失效，即在每千小时内，只允许有百万分之一的失效概率。

② 失效率的等级。

在失效率为常数的情况下，可以采用失效率的基准单位，将产品的失效率水平区分为若干等级。

我国于 1979 年发布了国家标准 GB/T 1772-79 《电子元器件失效率试验方法》，对有可靠性指标（ER）的军用元件，规定了失效率等级，该国标是参照了美军标 MIL-STD-690B（1968）而制定的，一直沿用到 20 世纪 90 年代初期。1996 年发布了国家军用标准 GJB 2649-96，该标准等效采用了美军标 MIL-STD-690C（1993），此后国军标有可靠性指标的元件将主要采用 GJB 2649-96 的相关规定。但目前大多数列入合格产品目录（QPL）中有可靠性指标的元件，仍沿用 GB/T 1772-79 规定的失效率等级，两者的失效率等级代号很容易混淆，现将这两个标准失效率等级的分类及代号同时列于表 2-3 中，以供比较。

表 2-3 失效率等级

失效率等级名称	失效率等级代号		最大失效率 (1/h 或 1/10次)
	GB/T 1772-79	GJB 2649-96	
亚五级	Y	L	3×10 ⁻⁵
五级	W	M	10 ⁻⁵
六级	L	P	10 ⁻⁶
七级	Q	R	10 ⁻⁷
八级	B	S	10 ⁻⁸
九级	J	—	10 ⁻⁹
十级	S	—	10 ⁻¹⁰

2.2.2 产品的寿命特征量

一批产品中某一特定产品在失效发生之前，难以指出其寿命的确切值，但在掌握了一批产品寿命的统计规律后，就可以指出产品寿命小于某一阈值的概率，或产品寿命在某一阈值范围内的概率。在可靠性工作中，经常用平均寿命、寿命方差、可靠寿命、中位寿命以及特征寿命等作为衡量产品可靠性的尺度。

1. 平均寿命 (MTBF 或 MTTF)

对于不可修复的产品，平均寿命是指产品发生失效前的工作或储存时间的平均值，通常记作 MTTF (mean time to failure, 平均失效前时间)；对于可修复的产品，平均寿命是指两次相邻故障间工作时间的平均值，通常记作 MTBF (mean time between failure, 平均故障间隔时间)。产品平均寿命的理论值为产品寿命 T 的数学期望，其表达式为：

$$E(t) = \int_0^{\infty} t f(t) dt$$

对于指数分布，有 $MTBF = 1/\lambda$ 。

如何理解 MTBF 是近几年争论比较大的地方。MTBF 的理解可用图 2-5 形象地表示出来。

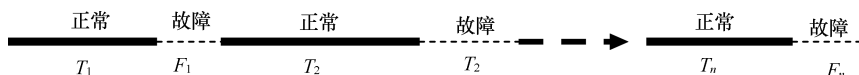


图 2-5 MTBF 示意图

在图 2-5 中， $MTBF = \sum_{i=1}^n T_i / n$ 。

MTBF 是产品平均故障间隔时间或者称为平均无故障工作时间。它是寿命为指数分布的产品的特征寿命。在试验中用 θ (如 GJB 899A 中) 或 m (如 GB 5080 中) 代替 MTBF。当产品工作到时间 $t=\theta$ 时，产品的可靠度只有 36.8%，即有 63.2% 的产品可能已经失效。MTBF 越大，表明产品的可靠性越高，其故障率就越小。

【例 2-5】时 MTBF 的理解

每天 24 小时连续运转的电梯，若要求其无故障工作的概率达到 $P(t)=99\%$ 以上，则电梯的 MTBF 必须大于 4500 小时。若要求其无故障工作的概率达到 $P(t)=99.9\%$ 以上，则电梯的 MTBF 必须大于 24000 小时。

【例 2-6】MTBF 与可靠度的关系

某产品平均故障间隔时间是一年 (MTBF=8760h)，有效使用时间是 24 小时，

那么，这个产品 24 小时的可靠度是多少？

$$R=e^{-\lambda t}=e^{-\frac{t}{MTBF}}=\exp(-24/8760)=0.99726$$

说明该产品在 24 小时内有 99.726%正常工作的概率。

对于指数分布，在规定的时间内，产品的 MTBF 与可靠度关系见表 2-4。

表 2-4 产品的可靠度与产品 MTBF 的关系

MTBF	可靠度（t=10h）	可靠度（t=1h）
10	0.3678794	0.9048374
100	0.9048374	0.9900498
1 000	0.9900498	0.9990005
10 000	0.9990005	0.9999000
100 000	0.9999000	0.9999900
1 000 000	0.9999900	0.9999990

2. 寿命方差与寿命标准离差

产品寿命 T 的方差称为产品的寿命方差，其理论值为：

$$D(t)=\int_0^{\infty} [t-E(t)]^2 f(t)dt$$

寿命方差的均方根，称为产品的寿命标准离差。

3. 可靠寿命

对于给定可靠度 r ，产品工作至可靠度为 r 的时间，称为可靠度为 r 的可靠寿命。若以 ρ_r 表示可靠寿命，则可从方程式 $R(\rho_r)=r$ 中求出 ρ_r 。

4. 中位寿命

产品工作到可靠度为 50%时的寿命时间，称为产品的中位寿命，显然此时有：

$$R(\rho_{0.5})=F(\rho_{0.5})=50\%$$

5. 特征寿命

产品工作到可靠度为 e^{-1} 时的寿命时间，称为产品的特征寿命，显然此时有：

$$R(\rho_{e^{-1}})=e^{-1}=36.8\%$$

6. 更换寿命

对于给定的失效率 λ ，当产品的失效率函数下降到低于给定的失效率水平的寿命时间时，称为产品的更换寿命，即对于给定的 λ 有：

$$\lambda(\rho_{\lambda}) \geq \lambda$$

则称 ρ_{λ} 为更换寿命。

7. B10 寿命

B10 寿命最早用于描述轴承的可靠性和寿命。轴承的可靠性是随其工作时间逐渐下降的，到了其耗损阶段，故障发生的频率会陡然增高，进入故障高发期。轴承的意外故障可能会带来较大的损失，为了减少意外故障的损失，需要在轴承进入耗损阶段之前就对其进行维修或更换，避免其进入故障高发期的耗损阶段。针对这个问题，人们提出一个非常朴素的做法：收集轴承的故障时间数据，通过统计方法得到 10% 的轴承发生故障的时间点，用 B10 表示这个时间点，如果轴承工作到这个时间点仍未失效（占 90% 左右），需要对其进行维修或更换。

B10 寿命是个产品的工作时间点，产品工作到这个时间点后，预期有 10% 的产品将会发生故障。

比 B10 寿命更广泛的描述为 BX 寿命，当 X 为 10 时称为 B10 寿命，当 X 为 5 时称为 B5 寿命。比较常见的 BX 寿命是 B0.1、B1、B5、B10、B50 寿命，对于汽车类产品，一般用 B10 寿命表达其整车和成件的可靠性。

假设某产品的故障累积函数（即不可靠度函数）为 $F(t)$ ，根据 B10 寿命的定义： $F(B10)=10\%$ ，则：

$$B10 = F^{-1}(0.1)$$

【例 2-7】可靠度、平均寿命、失效率的计算

某种手机（18 台）做寿命试验，各台发生失效的时间（单位：小时）为：160、290、506、680、1000、1300、1408、1632、1632、1957、1969、2315、2400、2912、4010、4315、4378、4500。

试求：（1）1000 小时的可靠度；（2）平均寿命；（3）500 小时的失效率， Δt 取为 10 小时。

解：我们用频率来近似概率。

（1）可靠度 = （工作到 1000 小时的台数） / （试验总台数），于是 $R(1000) = 14/18 = 77.78\%$ 。

（2）平均寿命 = （各台工作的时间总和） / [试验的总台数（因全失效）]，于是 $MTTF = (160 + 290 + \dots + 4378 + 4500) / 18 = 2075.78h$ 。

（3） $\lambda(t) = [t \text{ 到 } t + \Delta t \text{ 的失效台数} / (\text{工作到 } t \text{ 的台数} \cdot \Delta t)]$ ，于是 $\lambda(500) = 1 / (16 \times 10) = 0.00625 / 10h$ （这是某时间点的失效率）。

（4）假定手机寿命服从指数分布，则： $\lambda = 1 / MTBF = 1 / 2075.78 = 0.000481747 / h = 0.00481747 / 10h$ （这是平均的失效率，指数分布时失效率为常数，参见第 2.3.1 节）。

2.2.3 可靠性参数间的相互关系

由产品可靠性参数的基本概念可以看出：产品的可靠度与失效分布函数（参见第 2.3 节）之间为互逆关系，产品失效分布函数与分布密度函数之间为微积分关系，因此可以构成如图 2-6 所示的关系图。

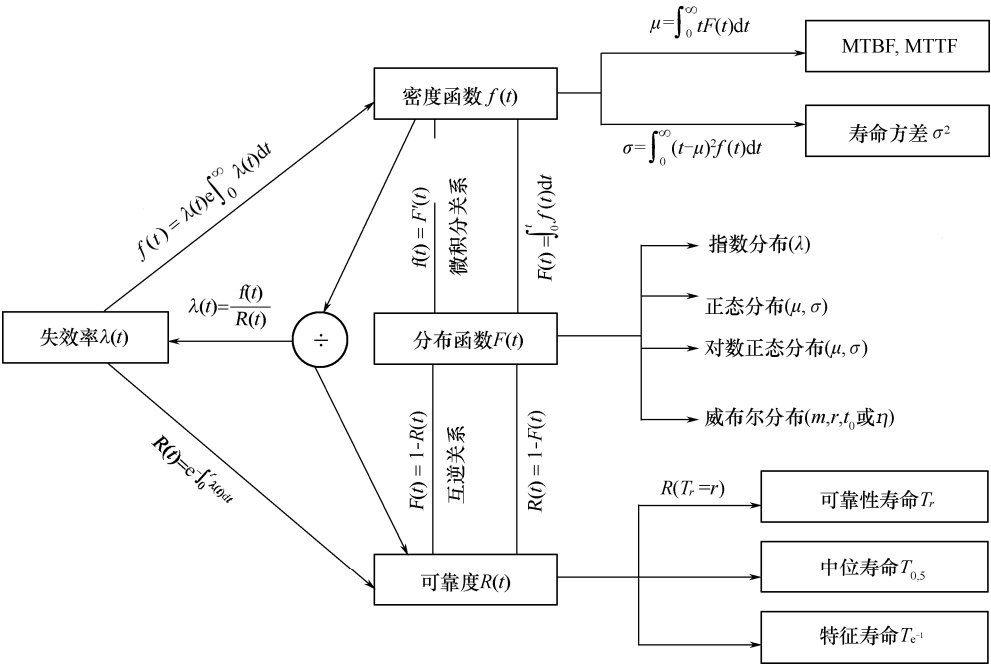


图 2-6 可靠性参数间的相互关系

由图 2-6 可知，只要知道方框中 $R(t)$ 、 $F(t)$ 、 $f(t)$ 、 $\lambda(t)$ 这 4 个函数中的任何一个，就可以顺着箭头方向按相应的方程式，求出所有的可靠性参数。

所谓可靠性指标，就是根据产品使用需求对其可靠性应达到的水平的量化要求。可靠性指标一般使用可靠性参数的阈值来表述，可以是参数的上限、下限、置信区间等。

可靠性指标在形式上有可靠性使用参数、可靠性合同参数、目标值、门限值、规定值、最低可接受值等。图 2-7 描述了可靠性指标在产品寿命周期各阶段的时序关系。

1. 可靠性使用参数

直接反映对产品/系统使用需求的可靠性参数。其要求的量值称为可靠性使用指标（简称为使用指标），使用可靠性值表示。

2. 可靠性合同参数

在合同中描述订购方对系统可靠性要求的，并且是承包商在研制与生产过程中能够控制的参数。其要求的量值称为可靠性合同指标（简称为“合同指标”），一般用固有可靠性值表示。

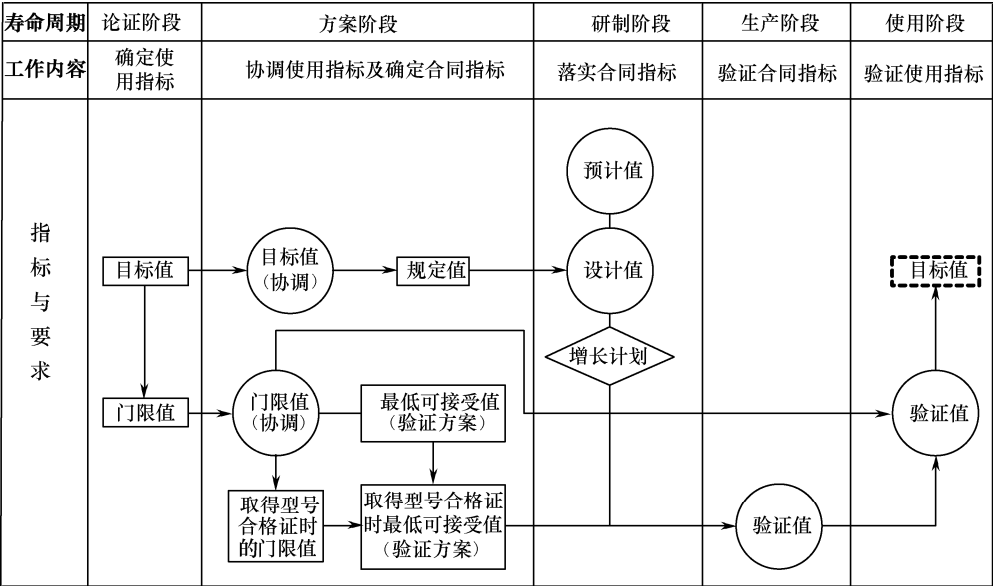


图 2-7 可靠性参数各量值的时序关系

3. 目标值

期望系统达到的使用指标，它既能满足使用需求，又可使系统达到最佳效费比，是确定规定值的依据。

4. 门限值

系统必须达到的使用指标，它能满足系统的使用要求，是确定最低可接受值的依据。

5. 规定值

合同中规定的期望系统达到的合同指标，它是承包商进行可靠性设计的依据。

6. 最低可接受值

合同中规定的、系统必须达到的合同指标，它是进行考核或验证的依据。

2.3 产品的寿命分布

在可靠性工作过程中，常常涉及产品的寿命分布问题，为了更好地理解产品的寿命分布含义，假设产品 A 的失效时间如图 2-8 所示。由图 2-8 可知，不同产品的寿命数据有不同的分布特点。图 2-8 (a) 的数据大多数都集中在这组数据的中心，具有中间大、两头小的分布特性；图 2-8 (b) 的数据大多数都集中在初始阶段，具有前面较密，后面稀疏的分布特性。如果将这两组数据的频率直方图连接成光滑的包络线，其特点就更加明显了。

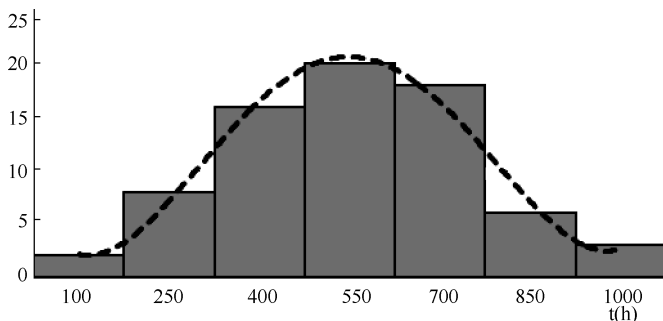


图 2-8 (a) 产品 A 寿命分布

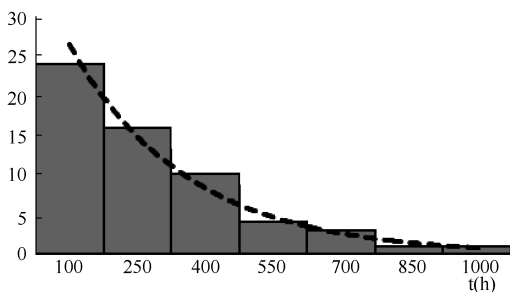


图 2-8 (b) 产品 B 的寿命分布

由图可见，图 2-8 (a) 的包络线呈钟型，图 2-8 (b) 的包络线呈滑坡下降型。事实上，用差分或差商方法对试验数据的类型进行判定，并对实验曲线进行滤波和光滑以后，图 2-8 (a) 的包络线可用如下解析式来表示：

$$f(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} \quad (2-7)$$

图 2-8 (b) 的包络线可用如下解析式来表示:

$$f(t) = \lambda e^{-\lambda t} \quad (2-8)$$

数学上将可用式 (2-7) 来表达其统计规律的分布称为正态分布。将可用式 (2-8) 来表达其统计规律的分布称为指数分布。

在可靠性实践中, 人们发现可以用指数分布、正态分布、对数正态分布、威布尔分布、超几何分布、伽马分布、贝塔分布、寿命分布来描述产品的失效分布规律。

2.3.1 指数分布

指数分布是可靠性实践中最常见的分布, 它的概率密度函数为:

$$f(t) = \lambda e^{-\lambda t}$$

式中, λ 称为失效率。服从指数分布的产品, 在早期失效阶段, 失效密度较高, 随着时间的推移, 失效密度逐渐降低, 并趋向恒定。

根据可靠性指标的相互关系, 可以得到:

$$F(t) = 1 - e^{-\lambda t} \quad (2-9)$$

$$R(t) = e^{-\lambda t}$$

$$\lambda(t) = \lambda$$

$$MTBF = \frac{1}{\lambda}$$

$$D(t) = 1/\lambda^2$$

$$\rho_r = -\ln(r)/\lambda$$

$$\rho_{0.5} = -\ln(2)/\lambda$$

$$\rho_{e^{-1}} = 1/\lambda$$

令 $MTBF = \theta$, 由上述结果, 并根据:

$$R(\theta) = e^{-\lambda\theta} = e^{-1} = 36.8\%$$

可以得出如下结论: 当产品服从指数分布时, 失效率近似为常数。其平均寿命、寿命标准离差和特征寿命都是失效率的倒数, 且产品工作到平均寿命 (MTBF) 时, 其可靠度为 36.8%, 因此, 对于服从指数分布的产品而言, 只要掌握了产品的失效率就可以知道产品的全部分布特性。

指数分布的一个重要性质是无记忆性。无记忆性是产品在经过一段时间 t_0 工作之后的剩余寿命仍然具有原来工作寿命相同的分布, 而与 t 无关 (马尔可夫特性)。

这个性质说明, 寿命分布为指数分布的产品, 过去工作了多久对现在和将来的寿命分布不发生影响。

【例 2-8】指数分布可靠度的计算

某计算机故障率是恒定的, 若平均每 3 个月发生一次错误, 设有一个需要 5 小时才能解决的问题, 问该计算机解决问题的可靠度是多少?

$$MTBF=3 \times 30 \times 24=2160\text{h}$$

$$\lambda=1/MTBF=1/2160=0.000463 \text{ 错误数/小时}$$

$$R(5)=e^{-\lambda t}=e^{-0.000463 \times 5}=0.99769$$

因此, 该计算机解决问题的可靠度是 0.99769。

2.3.2 正态分布

正态分布是一种应用极其广泛的分布, 其概率密度函数为:

$$f(t)=\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2}$$

我们定义 $\mu=0$, $\sigma=1$ 的正态分布为标准正态分布。对于标准正态分布的分布函数而言, 有:

$$\Phi(x)=\int_0^x \frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}dx$$

对于正态分布函数, 统计学和各种数学手册已有专门的数表可查。

若令 $X=\frac{t-\mu}{\sigma}$, 则有 $dx=\frac{dt}{\sigma}$, $t=\mu+\sigma x$ 。利用这种变换可以证明: 当产品寿命服从正态分布时, 式中参数 μ 就是产品的平均寿命, 参数 σ 就是产品的寿命标准离差, 而且产品的中位寿命同产品的平均寿命相等。

应用可靠性指标间的相互关系图, 可以得到产品的累积失效概率 $F(t)$ 、可靠度 $R(t)$ 、失效率函数 $\lambda(t)$ 、可靠寿命 ρ_r 、特征寿命 ρ_{e-1} 的计算公式为:

$$F(t)=\int_0^t \frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2}dt \quad (2-10)$$

$$=\int_0^{\frac{t-\mu}{\sigma}} \frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}dx=\Phi\left(\frac{t-\mu}{\sigma}\right)$$

$$R(t)=1-F(t)=1-\Phi\left(\frac{t-\mu}{\sigma}\right) \quad (2-11)$$

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{\Phi\left(\frac{t-\mu}{\sigma}\right)/\sigma}{1-\Phi\left(\frac{t-\mu}{\sigma}\right)}$$

$$\rho_r = \mu + \sigma K_{1-r}$$

$$\rho_{e^{-1}} = \mu + \sigma K_{0.632} = \mu + 0.34\sigma$$

式中, K_{1-r} 为标准正态分布的 $1-r$ 上侧分位点。

2.3.3 对数正态分布

当正态分布函数的自变量取对数时, 就变为对数正态分布函数。它的概率密度函数为:

$$f(t) = \frac{1}{\sigma t \sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{\ln t - \mu}{\sigma}\right)^2} \quad (2-12)$$

式中, μ 称为对数均值, σ^2 称为对数方差。

若以 $\varphi(x)$ 表示标准正态分布的概率密度函数, 以 $\Phi(x)$ 表示标准正态分布的分布函数, 以 K_{1-r} 表示标准正态分布函数的 $1-r$ 上侧分位点, 令 $x = \frac{\ln t - \mu}{\sigma}$, 则有

$dx = \frac{dt}{\sigma t}$, $\ln t = x\sigma + \mu$ 。根据上述关系式, 利用可靠性指标间的相互关系图, 可以证明: 对数正态分布的分布函数 $F(t)$ 、可靠度 $R(t)$ 、失效率 $\lambda(t)$ 、平均寿命 $E(T)$ 、寿命方差 $D(T)$ 、可靠寿命 ρ_r 、中位寿命 $\rho_{0.5}$ 、特征寿命 $\rho_{e^{-1}}$ 的计算公式为:

$$\begin{aligned} F(t) &= \int_0^t \frac{1}{\sigma t \sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{\ln t - \mu}{\sigma}\right)^2} dt \\ &= \int_0^{\frac{\ln t - \mu}{\sigma}} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx = \Phi\left(\frac{\ln t - \mu}{\sigma}\right) \end{aligned} \quad (2-13)$$

$$R(t) = 1 - \Phi\left(\frac{\ln t - \mu}{\sigma}\right) \quad (2-14)$$

$$\lambda(t) = \frac{\varphi\left(\frac{\ln t - \mu}{\sigma}\right)/\sigma t}{1 - \Phi\left(\frac{\ln t - \mu}{\sigma}\right)}$$

$$E(T) = e^{\mu + \frac{\sigma^2}{2}}$$

$$D(T) = e^{2\mu + \sigma^2} [e^{\sigma^2} - 1]$$

$$\rho_r = e^{\mu + \sigma K_{1-2}}$$

$$\rho_{0.5} = e^{\mu}$$

$$\rho_{e^{-1}} = e^{\mu + 0.34\sigma}$$

2.3.4 威布尔分布

瑞典的威布尔在研究链的强度时，构造了一种分布函数。后来人们发现，凡属由于局部失效而导致整体机能失效的串联式模型都能采用这种分布函数来进行描述。这种分布函数具有普遍意义并得到了广泛的应用，尤其适用于机电类产品磨损失效的分布规律描述，并被人们称之为威布尔分布函数。威布尔分布函数的形式为：

$$F(t) = 1 - e^{-\left(\frac{t-\gamma}{t_0}\right)^m} \quad (2-15)$$

其概率密度函数为：

$$f(t) = \frac{m}{t_0} (t - \gamma)^{m-1} \cdot e^{-\frac{(t-\gamma)^m}{t_0}} \quad (2-16)$$

式中， m 称为形状参数， γ 称为位置参数， t_0 称为尺度参数。

令 $\eta = t_0^{\frac{1}{m}}$ ，则称 η 为真尺度参数。令 $\Gamma\left(1 + \frac{1}{m}\right) = \int_0^\infty u^{\frac{1}{m}} e^{-u} du$ ，则称 $\Gamma(x)$ 为伽玛函数。这种函数在数学手册中有表可查。如果设 $u = \frac{t^m}{t_0}$ ，则有 $du = m \frac{t^{m-1}}{t_0} dt$ ， $t = (ut_0)^{1/m}$ 。根据这些关系式，利用可靠性指标的相互关系图，可以证明：当 $\gamma=0$ 时， η 就是产品的特征寿命，而且其可靠性 $R(t)$ 、失效率 $\lambda(t)$ 、平均寿命 $E(T)$ 、寿命方差 $D(T)$ 、可靠寿命 ρ_r 、中位寿命 $\rho_{0.5}$ 的计算公式为：

$$R(t) = e^{-\frac{t^m}{t_0}} \quad (2-17)$$

$$\lambda(t) = \frac{m}{t_0} t^{m-1} \quad (2-18)$$

$$E(T) = \eta \Gamma\left(1 + \frac{1}{m}\right)$$

$$D(T)=\eta^2\left\{\Gamma\left(1+\frac{2}{m}\right)-\Gamma^2\left(1+\frac{1}{m}\right)\right\}$$
$$\rho_r=\eta(-\ln r)^{1/m}$$
$$\rho_{0.5}=\eta(\ln 2)^{1/m}=\eta(0.693)^{1/m}$$

如前所述，威布尔分布能体现产品全寿命期的失效特征，包括早期失效期、偶然失效期和耗损失效期；威布尔分布的一个重要参数是形状参数 m ：

- $m<1$ 时：表示产品处于早期失效期。
- $m=1$ 时：表示产品处于偶然失效期。
- $m>1$ 时：表示产品处于耗损失效期。

威布尔分布的适用范围较广，服从指数分布、正态分布的产品同样可以用威布尔分布来描述：

- 当 $m=1$ ， $\gamma=0$ 时，代表指数分布，式中 t_0 即为平均寿命。
- 当 $m=3.4$ 时，接近正态分布。

【例 2-9】轴承 B10 寿命计算

某轴承的故障统计数据如表 2-5 所示，我们来计算它的 B10 寿命。

表 2-5 某轴承的故障统计数据

序号	工作时间（小时）	事件	序号	工作时间（小时）	事件
1	158	故障	11	887	故障
2	387	故障	12	964	故障
3	527	故障	13	981	故障
4	562	故障	14	994	故障
5	621	故障	15	996	故障
6	680	退出	16	1182	故障
7	754	退出	17	1224	退出
8	797	故障	18	1313	故障
9	801	故障	19	1322	故障
10	854	退出	20	1479	故障

我们在前面已经定义了 B10 寿命，即：B10 寿命是一个产品的工作时间点，产品工作到这个时间点后，预期有 10%的产品将会发生故障。

假设某产品的故障累积函数（也可以称为不可靠度函数）为 $F(t)$ ，根据 B10 寿命的定义： $F(B10)=10\%$ ，则：

$$B10=F^{-1}(0.1)$$

$$\int_0^{B10} f(t)dt = 10\% \quad (2-19)$$

轴承的寿命分布一般服从威布尔分布, 因此, 我们采用威布尔分布描述轴承的寿命特征。下面求其 B10 寿命。

当 $X=10$, $F=0.1$ 时, 综合式 (2-18) 和式 (2-19) 得到:

$$B10 = \eta e^{\frac{\ln \ln \left(\frac{1}{1-10\%} \right)}{m}} = \eta e^{\frac{-2.25}{m}} \quad (2-20)$$

进一步, 当产品的寿命服从指数分布时 (即当 $m=1$ 时), 这时 $MTBF=\eta$, 于是有:

$$B10=0.10536MTBF$$

利用下式的威布尔分布函数对表 2-5 的数据进行数据拟合, 可以得到两个参数, 分别为 $\eta=1090(h)$, $m=2.19$:

$$F(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^m}$$

利用式 (2-20) 可以得到 B10 寿命点估计值 $\hat{B10}$:

$$\hat{B10} = \eta e^{\frac{\ln \ln \left(\frac{1}{1-10\%} \right)}{m}} = \eta e^{\frac{-2.25}{m}} = 1090 \times e^{\frac{-2.25}{2.19}} = 390.2(h)$$

计算置信度为 80% 时该轴承的 B10 寿命的下限估计值 $\hat{B10}_L$:

$$m_1 = \ln[-\ln(1-10\%)] = \ln[-\ln(0.9)]$$

$$Q_1 = e^{\frac{\delta_1 + m_1}{\hat{m}}} = 0.8124$$

$$\hat{B10}_L = Q_1 \times \hat{B10} = 0.8124 \times 390.2 = 317(h)$$

2.3.5 超几何分布

超几何分布的概率计算在抽样方案设计中是计算接收概率的基础, 非常重要。

超几何分布常用于连续事件导致系统失效的情况建模。考虑一个具有隐含冗余配置的系统, 当两个连续器件发生失效时将导致系统失效, 在这种情况下系统的可靠度可用超几何分布来进行建模。假设 N 件产品中有 M 件为次品, 从中任取 $n(n \leq M)$ 件产品, 设其中次品数为 X , 则称 X 服从超几何分布。若 X 服从超几何分布, 则其分布为:

$$P\{X=k\} = \frac{C_M^k C_{N-M}^{n-k}}{C_N^n} \quad (k=0,1,2,\dots,n) \quad (2-21)$$



期望和方差分别为：

$$E(X) = n \left(\frac{k}{N} \right)$$

$$D(X) = n \left(\frac{k}{N} \right) \left(\frac{N-k}{N} \right) \left(\frac{N-n}{N-1} \right)$$

由于概率分布的表达式与“超几何函数”的级数展开系数有关，故称之为超几何分布。这就说明超几何分布的极限是二项分布。在实际应用时，只要 $N \geq 10n$ ，就可用二项分布近似计算超几何分布的有关问题。

2.3.6 伽马(Γ)分布

伽马分布可以表示较大范围的失效率函数，包括递减失效率函数、常数失效率函数及递增失效率函数。这种分布模型适用于描述期间失效分为 n 个阶段发生的情况，或者由于一个系统的 n 个独立的子器件失效导致整体失效的情况。

若随机变量 X 具有概率密度：

$$f(x) = \begin{cases} \frac{\lambda^\alpha}{\Gamma(\alpha)} x^{\alpha-1} e^{-\lambda x} & x \geq 0 \\ 0 & x < 0 \end{cases} \quad (2-22)$$

其中， $\alpha > 0, \beta > 0$ ，则称 X 服从参数为 α, β 的伽马分布，记为 $X \sim \Gamma(\alpha, \beta)$ ； α 称为形状参数， β 称为尺度参数； $\Gamma(\alpha)$ 称为伽马函数，其表达式为： $\Gamma(\alpha) = \int_0^\infty x^{\alpha-1} e^{-x} dx$ 。

累积分布函数 $F(x)$ 为：

$$F(x) = I\left(\frac{x}{\beta}, \alpha\right)$$

其中， $I\left(\frac{x}{\beta}, \alpha\right)$ 称为不完全伽马函数，其取值表由 Pearson 完成。可靠度函数 $R(t)$ 为：

$$R(t) = \int_t^\infty \frac{1}{\beta \Gamma(\alpha)} \left(\frac{\tau}{\beta}\right)^{\alpha-1} e^{-\frac{\tau}{\beta}} d\tau \quad (2-23)$$

当形状参数 a 为整数 n 时，伽马分布即为 Erlang 分布，这种情况下，累计分布函数表示为：

$$F(t) = 1 - e^{-\frac{t}{\beta}} \sum_{k=0}^{n-1} \frac{\left(\frac{t}{\beta}\right)^k}{k!} \quad (2-24)$$

失效率函数为:

$$h(t) = \frac{\frac{1}{\beta} \left(\frac{t^{n-1}}{\beta} \right)}{(n-1)! \sum_{k=0}^{n-1} \frac{\left(\frac{t}{\alpha} \right)^k}{k!}} \quad (2-25)$$

【例 2-10】某供电系统可靠性的特征量计算

某系统需要恒定电流供电, 电流由一个主电池提供, 同时备有 2 个相同的备份电池, 主电池的寿命 T_1 服从均值为 100 小时的指数分布, 备份电池的平均寿命为 100 小时。当主电池失效时, 第一个备用电池开始供电, 当第一个备用电池失效时, 第二个备用电池开始供电。试计算该系统在 $t=280$ 小时时的可靠度函数和失效率函数, 并求该系统的平均寿命。

解: 每个电池的寿命相互独立, 均服从均值为 100 小时的指数分布, 则系统的寿命分布服从 $\alpha=3, \beta=100$ 的伽马分布, 代入式 (2-23) 有:

$$R(280) = e^{-\frac{280}{100}} \sum_{k=0}^2 \frac{\left(\frac{280}{100} \right)^k}{k!} = 0.4014$$

280 小时的失效率可代入式 (2-25) 计算得到:

$$h(280) = \frac{\frac{1}{100} \left(\frac{280^2}{100} \right)}{2! \sum_{k=0}^2 \frac{\left(\frac{280}{100} \right)^k}{k!}} = 0.008812$$

系统的平均寿命:

$$E(x) = \alpha\beta = 300 \text{ (小时)}$$

2.3.7 贝塔分布

当产品或组件的寿命可能是限制在一个时间段中时, 贝塔分布最适合描述产品在 $(0, 1)$ 区间内的可靠度。像其他寿命分布的函数都可以描述三种形式的失效率函数——递减、恒定、递增的失效率一样, 贝塔分布的前两个参数也使其可以灵活地描述失效率的特性。贝塔分布的概率密度函数的标准形式如下。

如果 X 服从连续分布的概率密度函数为:

$$f(x|\alpha\beta) = \begin{cases} \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1} (1-x)^{\beta-1} & 0 < x < 1 \\ 0 & \text{其他} \end{cases} \quad (2-26)$$

则称随机变量 X 服从带参数 α 和 β 的贝塔分布 ($\alpha > 0, \beta > 0$)。

由于 $\int_0^1 f(x)dx = 1$ ，因此：

$$\int_0^1 x^{\alpha-1}(1-x)^{\beta-1} dx = \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}$$

一般情况下，累积分布函数和失效率函数没有解析表达式，但如果 α, β 是正整数，利用二项式展开的方法可以得到 $F(t)$ ，进而得到 $h(t)$ 。 $F(t)$ 是关于 t 的多项式， t 的阶数在一般情况下是介于 $0 \sim (\alpha + \beta - 1)$ 的正实数。

贝塔分布的均值和方差分别为：

$$E(x) = \frac{\alpha}{\alpha + \beta}$$

$$D(x) = \frac{\alpha\beta}{(\alpha + \beta)^2(\alpha + \beta + 1)}$$

当参数 $\alpha = 1, \beta = 1$ 时，贝塔分布是 $(0,1)$ 区间上的均匀分布。

2.3.8 寿命分布

开展可靠性工作时，掌握相应的寿命分布是基础。表 2-6 给出了常用的寿命分布的分布函数、概率密度函数、失效率计算公式以及随机抽样函数。其中，随机抽样函数在可靠性仿真，例如蒙特卡洛仿真中使用较多。

表 2-6 寿命分布的计算模型及随机抽样函数

类 型	分布函数	概率密度函数	失效率计算公式	随机抽样函数
指数分布	$1 - e^{-\lambda t}$	$\lambda e^{-\lambda t}$	λ	$-\frac{1}{\lambda} \ln(1 - \eta)$ 或 $-\frac{1}{\lambda} \ln \eta$ 式中， η 为 $[0,1]$ 的随机数
标准正态分布	$\Phi(t)$	$\frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}}$	$\frac{\Phi(t)}{1 - \Phi(t)}$	$\sqrt{-2 \ln \eta_1} \cos 2\pi \eta_2$ 或 $\sqrt{-2 \ln \eta_1} \sin 2\pi \eta_2$ 式中， η_1 和 η_2 均为 $[0,1]$ 的随机数
正态分布	$\Phi\left(\frac{t - \mu}{\sigma}\right)$	$\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t - \mu}{\sigma}\right)^2}$	$\frac{\Phi\left(\frac{t - \mu}{\sigma}\right) / \sigma}{1 - \Phi\left(\frac{t - \mu}{\sigma}\right)}$	$\sigma t_{N01} + \mu$ 式中， t_{N01} 为标准正态分布的随机抽样函数
对数正态分布	$\Phi\left(\frac{\ln t - \mu}{\sigma}\right)$	$\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{\ln t - \mu}{\sigma}\right)^2}$	$\frac{\varphi\left(\frac{\ln t - \mu}{\sigma}\right) / \sigma}{1 - \Phi\left(\frac{\ln t - \mu}{\sigma}\right)}$	$\exp(\sigma t_{N01} + \mu)$ 式中， t_{N01} 为标准正态分布的随机抽样函数
威布尔分布	$1 - e^{-\left(\frac{t - \gamma}{t_0}\right)^m}$	$\frac{m}{t_0} (t - \gamma)^{m-1} \cdot e^{-\frac{(t - \gamma)^m}{t_0^m}}$	$\frac{m}{t_0} t^{m-1}$	$t_0 (-\ln \eta)^{\frac{1}{m}} + \gamma$ 式中， η 为 $[0,1]$ 的随机数

另外，由于不同的产品服从的分布类型各异，在确定、选用产品的适用分布时，需要注意以下几点：

- 分布类型往往与产品的类型无关，而与施加的应力类型、产品的失效机理和失效模式有关。常见的分布类型包括上述介绍的指数分布、正态分布、对数正态分布、威布尔分布、超几何分布、伽马分布、贝塔分布等。
- 指数分布在可靠性工作中广泛应用，一般情况下，电子产品的寿命试验和复杂系统的失效时间均可用指数分布来描述，但是不能什么产品都直接套用指数分布进行计算，否则计算结果将产生较大的误差。
- 在选用分布类型时，一般可采用失效物理检验（或者通过寿命试验）、数理统计方法确定产品的分布类型。其中，失效物理的方法更为准确，但是实现的技术难度及经费较高；可利用数理统计方法判断其分布，在当前可靠性工程中应用较广。

典型分布的产品类型适用范围举例，如表 2-7 所示。

表 2-7 常用产品寿命分布类型对照表

分布类型	适用范围
指数分布	具有恒定故障率的部件，无冗余度的复杂系统，经过试验并进行定期维修的部件
威布尔分布	某些电容器、滚珠轴承、继电器、开关、断路器、陀螺、电动机、电子管、电位计、航空发动机、电缆、蓄电池、材料疲劳等
对数正态分布	电机绕组绝缘、半导体器件、硅晶体管、锗晶体管、直升机旋翼叶片、飞机结构、金属疲劳等
正态分布	飞机轮胎磨损及某些机械产品

参 考 文 献

[1] 曹晋华，程侃. 可靠性数学引论. 北京：高等教育出版社，2006.

[2] 王自力. 可靠性维修性保障性要求论证. 北京：国防工业出版社，2011.

[3] 陈云翔. 可靠性与维修性工程. 北京：国防工业出版社，2007.

[4] 王正，谢里阳. 机械时变可靠性理论与方法. 北京：科学出版社，2012.

[5] GJB 451A-2005. 可靠性维修性保障性术语.

第3章

可靠性管理

3.1 可靠性管理概述

3.1.1 可靠性管理的概念

可靠性是产品的设计特性，是在设计中赋予、生产中实现、管理中保证、使用中发挥的产品固有属性。可靠性管理是指为确定和满足产品可靠性要求进行的一系列组织、计划、协调、监督等工作。为了保证产品可靠性要求的实现，对其实行全寿命周期管理至关重要。可靠性管理是发展高可靠性产品的基本保证，也是一项对产品质量建设及其效能发挥有着全局性影响的工作。

可靠性管理的内涵包括时间、对象、内容、组织机构等 4 个维度，如图 3-1 所示。

- 时间：可靠性管理的时间阶段。可靠性管理覆盖产品的整个寿命周期，包括论证阶段、方案阶段、工程研制与定型阶段、生产阶段与使用阶段等。
- 对象：可靠性管理的对象，如航天产品、航空产品、电子产品、特定型号产品、元器件的可靠性管理等。当不指明对象时，可认为管理对象是普适的，即适用于任何对象。
- 内容：可靠性管理的实施内容，包括制订可靠性管理规范 and 文件、制订可靠性工作计划、进行可靠性活动的组织协调、实施可靠性过程监督、控制和评审等。
- 组织机构：实施管理的主体，包括单位常设的管理机构（如质量处、可靠性中心）、上一级管理机构（如集团公司的质量部）、型号产品可靠性管理组织（如型号可靠性组）、试验评价管理组织（如可靠性试验中心）、故障归零管理组织（如故障审查组织）等。

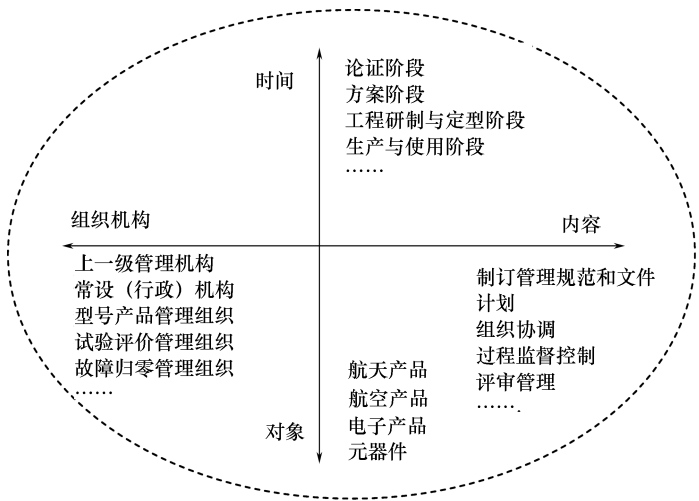


图 3-1 可靠性管理的维度

3.1.2 可靠性管理的基本职能

可靠性管理的基本职能是通过制订计划，建立或明确可靠性工作的组织机构和职责，对整个寿命期中的各项可靠性活动进行监督、控制和指导，以尽可能少的经费投入，实现规定的可靠性要求。

1. 计划

计划，即对产品全寿命周期的可靠性工作进行全面规划，确定可靠性目标，以及为达到此目标而采取的方针、方法、准则和需求的资源，以解决可靠性工作做什么、谁来做、何时做、如何做等问题。计划包括可靠性计划和可靠性工作计划。

2. 组织

组织，即建立由各级工程管理、技术部门和人员组成的可靠性管理组织机构，明确组织机构中科研计划、质量管理、技术培训等部门，以及各成员之间的关系、职责和权限，逐级落实可靠性管理和技术责任制。

3. 协调

为了实现管理的目标以达到规定的可靠性要求，可靠性管理组织应依据计划的方针、方法、准则、程序和资源，协调各部门以及各成员的工作，保证可靠性工作的有序开展。



4. 监督与控制

监督与控制，即对各项可靠性指标的完成情况进行检查，并将检查结果与预定要求进行比较，若偏差较大，则应采取控制措施。

3.1.3 可靠性管理的基本原则

为了更好地开展各项可靠性活动，可靠性管理应遵循和贯彻以下基本原则：

- 可靠性是影响产品使用和任务成功的重要质量特性，必须将可靠性置于与技术性能同等重要的位置看待，把各项可靠性工作作为重要任务认真对待，给予高度重视。
- 可靠性工作贯穿产品的寿命始终，应以全寿命的观点规划开展的可靠性工作，论证、方案、工程研制、定型、生产和使用等阶段的可靠性工作各有侧重，但同等重要。
- 可靠性管理是系统工程管理的重要组成部分，可靠性工作应与相关专业（如维修性、综合保障等）工作综合考虑，统筹规划，统一纳入产品的整个研制程序。
- 可靠性工作必须贯彻相关法规，执行相关标准，通过规范化的技术和管理途径，实现预定目标。
- 可靠性管理应强调从上层抓起，突出重点；安排可靠性工作时应遵循预防为主、早期投入的方针；应重视和加强可靠性信息的管理和利用等。

3.1.4 可靠性管理的内容

可靠性工作涉及产品寿命周期各阶段和系统各层次，包括要求确定、监督与控制、设计与分析、试验与评价，以及使用阶段的评估与改进等各项可靠性活动。表 3-1 是 GJB 450A《装备可靠性工作通用要求》给出的可靠性工作项目应用矩阵，明确了产品寿命周期各阶段应开展的可靠性工作项目，军工产品应据此剪裁执行，民用产品也可参照执行。

表 3-1 可靠性工作项目应用矩阵表

编号	可靠性工作项目类别	可靠性工作项目名称	论证阶段	方案阶段	工程研制与定型阶段	生产与使用阶段
1	可靠性及其工作	确定可靠性要求	√	√	×	×
2	项目要求的确定	确定可靠性工作项目要求	√	√	×	×
3	可靠性管理	制订可靠性计划*	√	√	√	√

(续表)

编号	可靠性工作项目类别	可靠性工作项目名称	论证阶段	方案阶段	工程研制与定型阶段	生产与使用阶段
4	可靠性管理	制订可靠性工作计划*	△	√	√	√
5		对承制方、转承制方、供应方的监督和控制*	△	√	√	√
6		可靠性评审*	√	√	√	√
7		建立故障报告、分析和纠正措施系统*	×	△	√	√
8		建立故障审查组织*	×	△	√	√
9		可靠性增长管理*	×	√	√	○
10	可靠性设计与分析	建立可靠性模型	△	√	√	○
11		可靠性分配	△	√	√	○
12		可靠性预计	△	√	√	○
13		故障模式、影响及危害性分析	△	√	√	△
14		故障树分析	×	△	√	△
15		潜在通路分析	×	×	√	○
16		电路容差分析	×	×	√	○
17		制定可靠性设计准则	△	√	√	○
18		元器件、零部件和原材料的选择与控制	×	△	√	√
19		确定可靠性关键产品	×	△	√	○
20		确定功能测试、包装、储存、装卸、运输和维修对产品可靠性的影响	×	△	√	○
21		有限元分析	×	△	√	○
22		耐久性分析	×	△	√	○
23	可靠性试验与评价	环境应力筛选	×	△	√	√
24		可靠性研制试验	×	△	√	○
25		可靠性增长试验	×	△	√	○
26		可靠性鉴定试验	×	×	√	○
27		可靠性验收试验	×	×	△	√
28		可靠性分析评价	×	×	√	√
29	使用可靠性评估与改进	寿命试验	×	×	√	△
30		使用可靠性信息收集	×	×	×	√
31		使用可靠性评估	×	×	×	√
32		使用可靠性改进	×	×	×	√

符号说明：“√”表示适用；“△”表示可选用；“○”表示仅设计更改时适用；“×”表示不适用

备注：可靠性工作项目名称中带“*”者，本身属于可靠性管理子项目

可靠性管理是从系统的观点出发,对产品寿命周期中各项可靠性活动进行规划、组织、协调与监督,以全面贯彻可靠性工作的基本原则,实现既定的可靠性目标。从整体而言,可靠性管理可分为宏观管理与微观管理。

- 可靠性宏观管理的内容包括:制定和贯彻国家标准与专业标准,组织有关的可靠性工作与管理机构,进行可靠性规划,规定可靠性考核指标,进行可靠性预先研究和基础研究,进行可靠性检查监督,组织可靠性情报的收集与交换,组织可靠性数据的收集与交换,开展行业协会、学会的可靠性技术交流,开展可靠性教育培训等。
- 可靠性微观管理是指产品研制单位在宏观管理的指导下,对其可靠性工作进行组织协调和保证。可靠性微观管理的内容包括:制订可靠性计划和可靠性工作计划;对承制方、转承制方、供应方的监督和控制;可靠性评审;建立故障报告、分析和纠正措施系统;建立故障审查组织;可靠性增长管理等。

本章所讨论的可靠性管理主要是指微观管理的有关内容。

制订可靠性计划和工作计划是可靠性管理的一项重要内容,以确定产品寿命周期各阶段的可靠性工作项目及其进度安排。开展可靠性工作需要相应的职能部门及明确的职责,确定职能部门及其职责是落实各项可靠性工作,实施有效可靠性管理的重要环节。此外,对可靠性工作进行监督与控制,实施可靠性评审,建立 FRACAS 和故障审查组织等是实施有效管理,确保实现规定可靠性要求的重要手段。这些管理项目所需的人力、经费和资源最少,一般应选用。

可靠性增长管理是一项复杂的技术管理工作。可靠性研制试验、可靠性增长试验和可靠性增长管理的目的都是为使产品的可靠性得到增长,并最终达到规定的可靠性要求。因此,应根据实际情况,权衡上述三项工作的效益和费用,选择最有效的途径实现可靠性增长。

3.1.5 可靠性管理与质量管理的关系

可靠性研究的目的是提高产品在规定条件下和规定时间内,完成规定功能的能力,或者说是研究在规定条件下,如何使得产品完成规定功能的时间更长。质量是一组固有特性满足要求的程度(ISO 9000:2000),就产品质量的好坏而言,主要包含技术性能、可靠性、经济性、安全性4个指标。

因此,产品的质量指标是一个综合性指标,可靠性指标是其中的一部分。然而,产品的可靠性研究又是质量管理工作的进一步发展和深化。一切质量工作除了要保证产品的性能、经济性和安全性之外,更重要的是要保证产品稳定可靠。从使

用的角度出发，产品的可靠性指标是其第一质量指标，是产品质量的核心内容。

广义而言，产品质量的优劣比较，其中必须包括产品可靠性水平的高低。根据有关资料介绍，国外在 20 世纪 70 年代已经发展到可靠性管理与质量管理二者互为补充、融合一体的质量保证体系。所谓质量保证体系就是产品在研究和设计阶段，运用固有技术和可靠性技术，奠定产品的可靠性等固有属性。生产阶段运用质量管理技术，使制造质量接近或达到设计水平。

可靠性管理的重点在于从产品的研究和设计阶段就保证固有技术和可靠性技术的实现，而制造过程中的可靠性保证可以利用现有质量管理体系，通过开展质量管理活动来实现，无须建立新的管理系统。这种产品制造过程中的质量管理与可靠性管理的兼容性，已被很多工厂的实践证明是保证产品质量和可靠性水平的有效方法。

可靠性管理与质量管理有着共同的目标，就是要使产品满足用户要求。二者既有联系也有差别，为了便于说明，现将可靠性管理与质量管理的差别列于表 3-2 中。

表 3-2 可靠性管理与质量管理的主要区别

项 目	质量管理	可靠性管理	关 系
目的	在允许的费用和一定的时间内生产出满足用户要求的产品，并以实现产品的低不良品率为主要目标	以最低限度的资源实现用户和产品计划所要求的规定时间 t 内的可靠性，即 $t>0$ 时的质量要求	目标一致，即满足客户要求
主要特点	一个过程，四大支柱（即标准化、PDCA、QC 小组、质量教育），四个环节（即 PDCA 循环），七种 QC 工具（即排列图、因果图、直方图、分层法、管理图、相关图、检查表），以及七种新 QC 工具（即关系图、KJ 法、系统图法、矩阵图法、PDPC 法、矢线图法、矩阵数据分析法）	一个基础（即可靠性组织），六大支柱（即可靠性设计、可靠性分析、可靠性评价、可靠性标准、可靠性数据、可靠性教育）	在可靠性设计分析中，同样可用 QC 工具，在现代质量分析中，同样会用到可靠性技术，如 FMEA、FTA 等
主要分工	质量控制、可靠性设计审查、可靠性教育、设计标准化、元器件筛选	可靠性管理、可靠性规划、可靠性、维修性、安全性、人机工程设计、各种指标的综合权衡、元器件管理与选用、失效分析、可靠性数据反馈、可靠性增长	在检验质量阶段，质量检验负责后端。在现代质量管理中，两者是融合的
	产品试验、检验、产品服务、外协厂管理		
所采用的主要手段	数理统计	同产品、材料、工艺有关的技术，可靠性物理，可靠性试验，数据统计技术	在现代质量管理中，两者是融合的
适用的阶段	批量生产	预研、设计、生产	良好的工艺质量是产品设计可靠性实现的基础和保证

(续表)

项 目	质量管理	可靠性管理	关 系
时间范畴	用时为 t 的阶段产品是否符合规范	研究产品在 $t>0$ 时 (使用时) 的质量 (可靠度), 可靠性又称为产品的时间质量	目标一致, 满足客户要求
对企业的经济效益	非常直接, 可在短期内提高成品率, 降低成本, 受企业欢迎	较为间接, 在短期内效果不一定显著地表现出来, 但长期坚持可给企业带来极大经济效益, 有利于国家安全和利益, 深受用户欢迎	提高可靠性是降低返修率的根本途径

3.2 可靠性计划与可靠性工作计划的制订

3.2.1 目的与作用

对于军工产品, GJB 450A 要求订购方制订可靠性计划, 承制方制订可靠性工作计划, 确保各项可靠性工作有计划、有组织、系统地实施。对于民用产品, 可将可靠性计划和可靠性工作计划的制订合并进行。

订购方制订可靠性计划的目的是: 全面规划装备在寿命周期内的可靠性工作, 通过制订并实施可靠性计划, 以合理的费用实现规定的可靠性使用要求, 满足战备完好性和任务成功性要求。

可靠性计划的作用包括:

- 对可靠性工作提出总要求, 做出总体安排。
- 对订购方应完成的可靠性工作做出安排。
- 明确对承制方可靠性工作的要求。
- 协调可靠性工作中订购方与承制方, 以及订购方内部的关系。

承制方制订可靠性工作计划的目的是: 通过制订和实施可靠性工作计划, 确保装备满足合同规定的可靠性要求。

可靠性工作计划的作用包括:

- 有利于从组织、人员、经费以及进度安排等方面保证可靠性要求的落实和管理。
- 反映承制方对可靠性要求的保证能力及其对可靠性工作的重视程度。
- 便于评价承制方实施控制可靠性工作的组织、资源分配、进度安排和程序是否合理。

3.2.2 计划的主要内容

不同产品的可靠性计划和工作计划，其内容和重点各不相同，究其共性内容，通常应回答以下问题：可靠性工作应达到的目标、需要开展的工作项目、如何开展、开展到何种程度、何时开始、何时结束、由谁负责实施等。计划还应明确有关可靠性管理机构（部门）、组织、人员在可靠性工作中的责任、权限和关系等。

具体而言，可靠性计划是订购方进行可靠性工作的基本文件，订购方应在装备立项综合论证时开始制订可靠性计划，其主要内容包括：

- 可靠性工作的总体要求和安排。计划中应描述装备的任务需求和使用要求（如战备完好性、任务成功性要求等），可靠性工作的总体目标、政策、原则及要求。
- 可靠性工作管理、实施机构及其职责。计划中应明确新建或委任装备可靠性工作的管理机构和实施机构，并说明其权限和职责。
- 可靠性及其工作项目要求论证工作的安排。计划中应明确可靠性要求论证工作的论证内容、原则、程序、方法、评审、进度、实施单位等要求。
- 使用可靠性评估与改进工作的要求和安排。计划中应明确使用可靠性信息收集计划、使用可靠性评估计划、使用可靠性改进计划的主要内容、实施过程及评价要求等。
- 对承制方监督与控制工作的要求和安排。计划中应明确对合同要求承制方开展的各项可靠性工作进行监督与控制的要求、内容、方法、时机等。
- 可靠性评审工作的要求和安排。可靠性评审是监督与控制的重要手段之一，由订购方主持的评审项目应在计划中明确承制方必须提供的资料文件要求等。
- 可靠性信息管理工作的要求和安排。可靠性信息是开展可靠性工作的基础，订购方除认真收集、分析、利用论证和使用阶段的可靠性信息外，还应当了解和掌握寿命周期其他各阶段必需的可靠性信息。为此，在计划和合同中应明确要求承制方提供的可靠性信息。
- 可靠性工作所需经费的预算说明。
- 工作进度等。

可靠性工作计划是承制方开展可靠性工作的基本文件。承制方应根据合同要求制订可靠性工作计划，并据此组织、指挥、协调、检查和控制其全部可靠性工作，以实现合同中规定的可靠性要求。可靠性工作计划的内容主要包括：

- 装备的可靠性合同要求和计划开展的可靠性工作项目，至少应包括合同要求的全部可靠性工作项目。此外，承制方为确保实现合同要求，亦可自行增加



其他可靠性工作项目。

- 每一项可靠性工作的实施细则，如实施的目的、要求、内容、方法、程度、完成形式、责任单位与人员、评审的节点和内容等。
- 可靠性管理机构、组织的职能和权限。
- 可靠性工作与相关专业工作相互协调，以及共用、传递信息的说明。
- 研制产品可靠性信息管理的要求、内容和方法说明。
- 开展可靠性工作所需的经费说明。
- 工作进度等。

以上可靠性工作计划的内容并非固定不变，应随着装备的研制不断完善，当订购方的要求发生变更时，可靠性工作计划也应做相应的更改，且应经评审和订购方认可。但无论计划的内容如何变更，均应包括：可靠性要求和可靠性工作项目要求；产品各阶段可靠性工作项目的实施细则；可靠性工作组织及人员；工作进度；每一阶段的节点，以及检查或评审点；可靠性信息的收集、传递、分析、处理、使用的程序及方法等内容。

3.2.3 编制可靠性计划与工作计划的一般要求

1. 可靠性计划与可靠性工作计划的关系

可靠性计划和可靠性工作计划分别是订购方和承制方进行可靠性管理的基本文件，两个计划的目标都是为最终实现装备完好性和任务成功性的要求，两个计划必须协调，承制方的可靠性工作计划必须符合订购方的可靠性计划要求，两个计划形成型号研制中可靠性管理的统一整体，以保证可靠性工作的顺利进行。

2. 制订可靠性工作计划的原则

- 可靠性工作计划应覆盖产品的整个寿命周期。
- 尽可能制定、实施各工作项目的日程表，以便审查计划的进展情况。
- 预算执行各项任务所需的设备、经费、时间，明确负责人的职责和权限。
- 应有定期检查计划执行情况的要求，必要时对计划进行补充和修正。

3. 制订可靠性工作计划应考虑的因素

可靠性工作计划是产品研制、生产计划的一部分，其内容应统一、协调。制订可靠性工作计划应考虑的因素包括：

- 产品可靠性水平的高低。产品可靠性要求越高，工作安排应越细，可靠性工作项目越多。

- 应针对产品研制的不同阶段，制定不同的工作项目。
- 考虑产品类型及同类产品的可靠性水平。不同类型产品的可靠性要求不同，适用的工作项目亦不同。
- 应统筹考虑产品研制的其他要求，如资金和进度等。

4. 计划的评审

应对可靠性计划和可靠性工作计划进行评审，可靠性工作计划还应得到订购方的认可。随着武器装备研制工作的进展，应结合研制节点对可靠性工作计划的执行情况进行检查和评审，以确定可靠性工作的有效性，及时发现问题并加以纠正。

5. 计划的监控

为保证计划目标的实现和各项可靠性工作按要求进行，必须对可靠性活动进行连续的跟踪与监督，及时了解计划的进展情况和出现的问题，给予及时指导和协调。应设立一系列监控点，对计划的进展情况进行评价和监控。可靠性计划一旦通过评审或确认后，订购方和承制方的可靠性管理机构必须运用调查、报告、检查、评审和考核等手段，对计划实施全过程的监督与控制，发现问题，修改完善计划。

6. 动态管理

随着研制工作的进展，可靠性计划和可靠性工作计划是需要不断调整 and 完善的，计划的修改，必须履行一定的报批手续，可靠性工作计划的修改还需要经订购方认可。

3.3 可靠性管理组织

产品可靠性是管理出来的，因此，先要组织落实，明确本部门或企业中可靠性管理机构的结构形式、职责权限、上下级部门，以及与其他职能机构之间的关系、协调方法。明确本部门或企业中主要可靠性管理机构的负责人，明确管理机构对产品可靠性的要求是以什么方式通知需要了解及执行的其他机构（技术、管理、工艺、生产等）人员，如何督促检查；明确其他机构、人员以什么方式向可靠性管理机构提供需要的信息等，因此，组织机构是管理的组织保证，应建立强有力的组织机构。

为了保证可靠性工作的各项措施自上而下的贯彻执行，有必要设置专职的可靠性管理机构，已经建立专职质量管理机构的单位，也可将可靠性管理职能纳入该机构。

可靠性组织可根据单位的情况安排，有的是将其与装备综合保障组织结合在一

起。设置专职的管理机构时，并非是包办一切可靠性工作。专职机构必须依靠和发挥各职能部门的作用，共同完成可靠性工程与管理任务。

3.3.1 研制、生产单位的可靠性管理组织

GB 6992《可靠性与维修性管理》推荐的可靠性管理机构的主要职责如下：

- 负责制订本单位可靠性等管理方针和计划，以最小的人力和投资，实现产品标准所规定的定量的可靠性等指标。
- 组织、协调和监督有关部门贯彻实施可靠性计划确定的各项任务。
- 指导可靠性主管师的工作。
- 组织进行可靠性设计评审。
- 组织元器件的质量认定或认证，实施元器件的统一管理。
- 组织有关的可靠性试验和失效分析。
- 组织可靠性数据、信息的收集与反馈。

某研制、生产单位的可靠性管理机构如图 3-2 所示，对其说明如下。

- 行政总指挥系统对产品研制的可靠性工作总体负责，并在计划、组织、协调和资源配置等方面保证可靠性工作的实施。
- 规划部门负责组织制订型号产品的研制工作计划，将可靠性工作统一纳入型号研制计划中，负责规划可靠性工作资源保障。
- 人力资源部门负责可靠性人力资源的配备，组织可靠性专业技术培训。
- 质量师系统负责组织实施产品研制中的质量与可靠性管理、监督工作。可靠性管理人员协助质量师对可靠性工作进行监督、控制，在对相关的技术文件、设计图样实施质量会签的同时审查其是否满足可靠性法规的标准要求。检查研制过程中可靠性工作计划的执行情况，参与重要试验和可靠性工作计划评审。对出现的技术质量问题和评审中提出的改进建议进行跟踪落实。
- 总设计师系统对产品研制过程中的技术总体负责，并负责产品的可靠性设计、分析、试验，以及可靠性技术方面的工作。
- 可靠性管理人员负责制订可靠性工作计划和设计准则，进行可靠性指标的预计和分配，协助设计人员完成各项可靠性试验工作；编制各类可靠性技术文件和资料，并负责收集、分析、审查和保存；参与监督可靠性工作计划的实施和评审；负责对可靠性数据的收集、整理与分析，并负责可靠性专业技术培训，为设计人员进行可靠性设计分析提供技术支持。
- 产品设计人员负责可靠性设计与分析工作，按照可靠性工作计划的要求，完

成规定的工作项目，严格执行可靠性标准、设计准则和设计规范，通过优化设计使产品达到规定的可靠性指标要求。

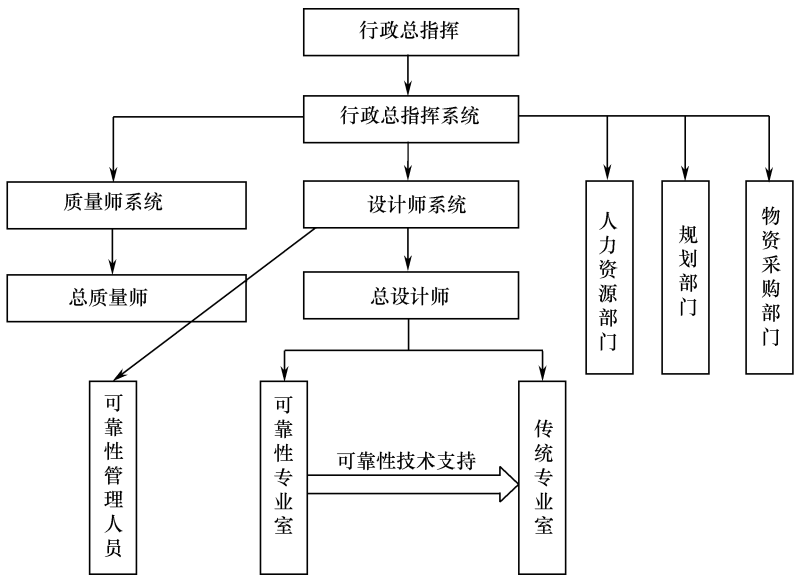


图 3-2 某研制、生产单位的可靠性管理机构

3.3.2 型号武器系统的可靠性管理组织

型号武器应当有可靠性管理组织，通常由型号总设计师负责项目可靠性工作，一名副总设计师主管可靠性工作。在其下设有可靠性管理组织，有可靠性主任或（和）主管设计师。分系统也应有类似的组织。有的行业将可靠性组织纳入质量工作系统，也有的是与装备综合保障组织结合在一起。

在研制、生产中，军方也要建立可靠性工作组织，其核心是军事代表系统。军事代表要把可靠性和装备综合保障作为质量监督与控制的最重要工作。GJB 3899A《大型复杂装备军事代表质量监督体系工作要求》规定，可以采取由军事代表局、处、室，组成型号军事代表质量监督体系，重点抓好可靠性工作。图 3-3 给出了某型号研制单位的可靠性组织机构示例。

1. 型号武器的可靠性工作系统职责

- 制定型号可靠性顶层设计文件和管理规定，包括可靠性工作计划、可靠性设计准则、元器件大纲等。
- 明确各级设计人员的职责：产品设计人员主要负责包括可靠性等所有设计质量特性的设计工作，专职可靠性人员负责可靠性方面的总体工作和技术



支援。

- 建立和实施有关图纸和技术资料的可靠性会签制度。

2. 可靠性总师职责

- 批准型号顶层的可靠性文件。
- 对型号可靠性的关键问题进行决策。
- 主持召开可靠性工作系统会议。
- 负责落实可靠性系统的活动经费。

3. 可靠性副总师职责

- 组织制订型号可靠性等工作目标、规划及工作制度，并组织落实。
- 组织编写型号可靠性指标的论证报告和可靠性工作计划。
- 组织或参与可靠性设计评审。
- 组织型号可靠性技术攻关和可靠性增长工作。
- 组织型号可靠性试验。
- 审批可靠性技术文件和技术报告。
- 组织型号可靠性技术培训。

4. 可靠性主任设计师职责

- 组织编写本单位产品的可靠性工作目标、规划及工作制度。
- 制订本单位产品的可靠性工作计划。
- 组织或参与本单位产品的可靠性设计分析工作。
- 组织或参与本单位产品的可靠性试验。
- 组织或参与本单位产品的可靠性评审。
- 组织管理本单位产品的各项可靠性工作，并及时向总师单位提交有关工作报告。
- 根据本单位的实际情况建立本单位的可靠性工作系统。
- 组织本单位有关人员进行可靠性技术培训。
- 代表本单位参加型号可靠性工作系统组织的可靠性活动。

5. 可靠性办公室主任职责

- 负责工作系统各单位之间的工作协调和联络。
- 负责工作系统内部各种会议的准备工作。
- 在总师和副总师的领导下，负责处理日常工作。

- 收集处理各成员单位提交的可靠性报告，将有关问题反馈给总师或副总师。

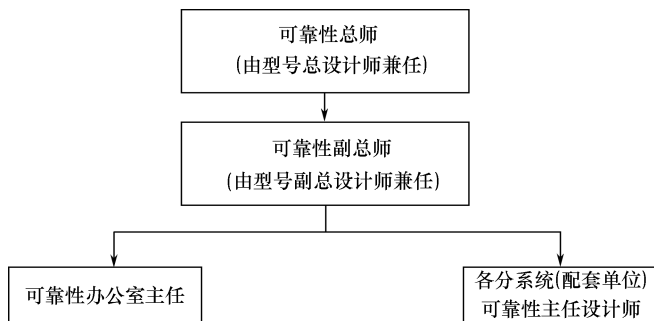


图 3-3 某型号可靠性管理机构示意图

3.4 可靠性过程管理

可靠性过程管理是指装备研制过程、生产过程、使用过程对可靠性工作的规划与管理，过程管理是可靠性管理的重要活动，它对保证可靠性要求的实现具有重要的意义。为此，质量管理人员、驻厂（所）质量监督（军事）代表应对承制方、转承制方和供应方的可靠性工作实施有效管理与监督。

3.4.1 研制阶段的可靠性管理

研制阶段是产品可靠性形成的关键阶段，实行研制过程的可靠性管理与监督，对产品可靠性水平的实现与减少寿命周期费用至关重要。

1. 研制阶段可靠性管理的意义

在产品的研制过程中，实施可靠性管理是可靠性工程活动的一项重要内容，其主要原因如下：

- 产品的可靠性首先决定于设计，而设计过程为产品的可靠性奠定基础，制造过程保证可靠性实现，维修过程维持可靠性水平。据统计，设计技术对产品可靠性水平的影响占比为 40%，制造技术对可靠性水平的影响占比为 10%，零件材料对可靠性水平的影响占比为 30%，而使用（运输、环境、安装、操作、维修技术）对可靠性水平的影响占比为 20%，因此，必须从设计开始就开展可靠性管理工作。
- 在产品的寿命周期费用中，设计及研制虽占全寿命周期费用的 15%，但它对



全寿命周期费用的影响却很大，由于实施了可靠性管理和开展可靠性活动，虽会少量增加设计及研制投资，但却能大量减少全寿命周期费用。

- 开展可靠性管理工作，通过试验和运行取得了信息，暴露了系统设计中的缺陷，然后通过再设计可以改进原有的设计方案，进而提高产品的可靠性水平。
- 我国可靠性工作起步较晚，很多产品没有认真进行可靠性设计，致使产品的可靠性水平较低，因此，从宏观和微观管理上，必须十分强调和重视设计过程的可靠性管理，大力开展可靠性设计工作。

2. 研制阶段可靠性管理的任务

研制阶段可靠性管理的主要任务是：根据确定的可靠性目标，制订可靠性工作计划；组织实施可靠性设计与分析、进行可靠性设计评审、可靠性试验、可靠性信息管理等。为了有效地实施可靠性管理，必须建立健全管理组织，型号产品应在设计师系统中设置可靠性（质量）工作系统、故障审查组织，并实行有效的控制与监督。

3. 研制各阶段的可靠性管理

（1）论证阶段的可靠性管理

- 使用方在进行装备战术技术指标论证的同时，应进行可靠性指标的论证。
- 任务招标单位应对国内外同类装备的可靠性水平进行分析，以便根据新的需求提出既先进又可行的指标。
- 提出装备的寿命剖面、任务剖面及其他约束条件，以及对这些指标的考核或验证方案的设想。
- 对可靠性经费需求进行风险分析。
- 在进行战术技术指标评审的同时，应对可靠性指标进行评审，最后纳入《研制总要求》中。

（2）方案阶段的可靠性管理

- 确订可靠性定性、定量要求及相应的考核或验证方法，并对其实施评审。
- 制订可靠性工作计划。
- 制订产品专用的可靠性规范、指南等技术文件。
- 建立故障报告、分析和纠正措施系统。
- 对产品的可靠性进行初步分析，并与费用、进度等因素进行综合权衡，确定达到定性、定量要求必须采取的技术方案。

- 在方案评审时，应将可靠性作为重点内容之一进行评审。
- 预算可靠性经费。

(3) 工程研制阶段的可靠性管理

在工程研制阶段，研制单位应实施可靠性工作计划，开展可靠性设计、分析和试验工作。完成试制任务后，对其可靠性进行验证。阶段评审时，应包括对实施可靠性工作计划的评审，具体应进行以下管理工作。

① 装备结构设计的管理。

根据基本方案进行具体的结构设计，并贯彻可靠性要求，对性能、可靠性、费用进行权衡。在某些情况下，宁可适当降低性能的要求以保证可靠性要求的实现。

② 进行可靠性的进一步分配。

将已经由系统分配至分系统、设备的指标分配至元器件与工艺，然后，再分配至每一个大类，即每一个元器件、结构件，以及导线、焊点、紧固点。不但要分配失效率，而且要分配生产制造过程中的不良率。

同时，还要进行部门的分配。从总体部门分配至设计、工艺、供应等各部门，直至每个工序和工位。分配的基本方法是“现场统计加修正”：现场统计是指将相似设备的制造和使用过程所积累的数据作为分配的基础；加修正是根据改进的可靠性进行必要的修正和协调，使分配更趋合理。

③ 组织进行初样机的可靠性设计。

在初样机的结构方案确定后，组织设计人员及可靠性工程师进行各项具体设计。可靠性设计的主要工作如下：

- 确定可靠性定量、定性要求及验证方案。
- 进行初样机可靠性建模与预计。
- 进行故障模式影响分析和故障树分析。
- 制订和贯彻可靠性设计准则。
- 制订和实施元器件大纲。
- 进行与软件有关的可靠性设计。
- 进行保障性安全性分析与设计。
- 正确处理可靠性设计与试验的关系。
- 建立并深化故障报告、分析与纠正措施系统。

④ 制订保障计划和保障方案。

应按 GJB 3872《装备综合保障通用要求》，依据保障方案和产品设计进展，制订保障计划，以影响产品设计。保障方案和保障计划的制订与完善为保障资源的协调与匹配提供了保证。



⑤ 进行可靠性分析。

根据实际条件,采用有关方案进行可靠性预计及安全性分析,同时进行FMECA及FTA等分析,检查是否能达到设计目标,及时发现设计中的薄弱环节,修改设计。最终的可靠性预计值必须大于或等于统计试验方案的上限值,保证在进行可靠性鉴定试验时以大概率通过。

⑥ 进行可靠性设计评审。

可靠性设计评审主要包括可靠性设计的先进性、经济性、可行性和可检验性,指出存在问题,提出解决建议和途径,并形成设计评审报告,设计评审报告应包括以下工作:

- 所采用的可靠性设计技术与实施方法是否已将可靠性设计指标设计到产品中,并可通过工艺实践能将其制造出来。
- 可靠性薄弱环节及其控制措施的有效性。
- 所采用的材料、结构和工艺能否保证产品的可靠性要求。
- 技术性能与可靠性是否同时得到了优化,达到满足设计指标的程度。

可靠性评审组还应对元器件的选择与降额应用、热设计、电磁兼容设计、漂移设计、“三防”设计、抗振设计、冗余设计、潜在电路分析、结构设计、机械概率设计、人机工程设计、失效安全设计、安全性设计、工艺设计等进行评审,以发现薄弱环节并进行改进。从当前的实际情况来看,元器件的选择与降额应用、工艺设计、电磁兼容设计及安全性设计是突出的薄弱环节,必须加强。

另外,对原理图、结构图、印制电路板图、可靠性预计与分析报告、新采用的元器件认定报告、关键电路、结构、工艺试验报告以及各项具体的可靠性设计文件要进行评审和会签,及时发现和纠正设计缺陷。

(4) 设计定型阶段的可靠性管理

在设计定型阶段主要考核型号武器的可靠性是否达到《研制任务书》和合同的要求。定型试验大纲要包括可靠性鉴定试验项目。组织定型评审时,对可靠性是否满足《研制任务书》和合同要求等进行评审。最后,将可靠性鉴定试验结果和可靠性工作计划的实施情况反映在定型文件中。

在设计定型阶段,还应进行以下主要管理工作。

- 组织元器件、组件、设备筛选。对于高可靠性产品以及重要的产品,对样机的元器件、组件、设备进行可靠性筛选,排除早期失效,并为制订正式的产品筛选条件提供依据。必须强调指出的是,进行筛选试验的样机,今后在生产中也必须进行同样的筛选,否则可靠性鉴定试验的结论是无效的。

- 组织样机的系统联试和现场试用。在环境试验和可靠性鉴定合格的条件下，组织样机的现场试用以及保障性鉴定试验，验证保障资源的匹配性及协调性。根据现场暴露的缺陷以及用户意见进一步改进设计与工艺。
- 组织设计定型的可靠性设计评审。根据可靠性设计报告、性能测试报告、环境试验报告、可靠性增长试验报告、可靠性鉴定试验报告、电磁兼容试验报告、原材料及元器件认定试验报告、现场和用户试用报告，以及设计、工艺文件，组织进行设计定型的可靠性评审，进一步完善设计及相应的文件，为批量试制生产做好准备。
- 根据 GJB 1362A《军工产品定型程序和要求》规定，在设计定型时，应在设计定型审查会议上提供可靠性分析评价报告。

(5) 生产定型阶段的可靠性管理

在生产定型阶段主要鉴定或评审批量生产条件下产品可靠性保证措施的有效性，以及技术状态的更改对其影响的研究和评审。管理的主要内容有：

- 应按合同规定的方法验证产品在批量生产条件下保证产品可靠性措施的有效性。
- 在生产过程中，加强质量控制；采取波动小的工艺技术；加强生产过程中环境应力筛选；当对零部件、工艺装备等技术状态更改时，必须分析其对可靠性的影响，并履行有关审批手续。
- 继续加强对转承制方和供应方的监控，以及外协件的人库检验。
- 在试生产、试验过程中，应使故障报告、分析和纠正措施系统（FRACAS）正常运行，促使产品可靠性继续增长。

3.4.2 生产阶段的可靠性管理

生产阶段的可靠性管理任务是进行生产过程的质量控制，确保生产出来的产品达到预期的可靠性水平。此阶段的主要工作有：

- 在生产过程中加强质量控制；采用成熟的工艺技术，加强生产过程对零部件、加工工序、工艺装备等质量管理，当技术状态更改时，必须分析其对产品可靠性的影响，并履行有关的审批手续。
- 继续加强对转承制方和供应方的监督及外协件的进厂复验。
- 确保在试生产、试用、批生产过程中，FRACAS 系统正常运行，促使产品的可靠性继续增长。
- 加强对保障资源的生产和配套性进行管理。

3.4.3 使用阶段的可靠性管理

使用阶段的主要任务是保持和发挥产品的固有可靠性水平。为此，必须做好以下工作：

- 使用方要完整、准确地收集产品现场使用和储存期间的可靠性信息，按规定向承制方反馈，并提出改进的意见和建议。
- 承制方按合同要求做好有关技术资料、备件供应、人员培训等技术服务工作。
- 进一步修订综合保障计划和综合保障工作计划。
- 依据保障方案、保障计划和保障资源建立保障系统，并根据现场使用评估结果，进行以下工作：
 - ◆ 调整人力和人员需求。
 - ◆ 调整备件和消耗品清单。
 - ◆ 进一步对保障设备进行改进，修订保障设置配套方案。
 - ◆ 修订相应的技术资料。
- 进一步修订训练或使用培训计划。
- 在装备部署前，做好以下工作：
 - ◆ 应基本完成保障设施的建造，以及装置部署到部队时，有足够的保障设施。
 - ◆ 应完成规划包装、装卸、储存和运输计划的实施工作。
 - ◆ 保证完成计算机资源保障计划的实施。
- 进行保障资源的试验与评价工作。

以上介绍了在产品不同阶段可靠性管理的主要工作内容，上述内容只是根据相关的可靠性标准，进行了探索性的展开讨论，仅供参考。在实际运用时，应根据装备的具体情况做相应的补充或剪裁。

3.4.4 对转承制方和供应方的监督与控制

监督与控制转承制方和供应方的目的是加强其在装备研制、生产工作中的协调，以保证可靠性符合装备或分系统的要求。为此在签订研制、生产合同时，承制方应根据产品的可靠性要求、复杂程度等提出对承制方和供应方的监督措施，并在

合同中应有承制方参与转承制方的重要活动（如设计评审、可靠性试验等），而对承制方、转承制方及供应方的监督是驻厂（所）质量监督（军事）代表必须进行的工作，质量监督（军事）代表应通过评审等手段进行监控承制方、转承制方和供应方的可靠性工作，评估各项工作项目的实施效果，以便尽早发现问题并采取必要的措施。

3.5 可靠性评审

可靠性评审是保证设计符合要求，由设计、生产、使用各部门代表组成的评审机构对产品的设计方案，从可靠性的角度，按事前确定的设计和评审表进行的审查，评审的主要目的是及时发现潜在的设计缺陷，加速设计的成熟，降低决策风险。

3.5.1 可靠性评审的作用

可靠性评审就是对可靠性工作计划的执行情况进行连续的观察与监控，以保证计划的全面实施，并达到预期目标。具体做法是在研制过程中，设置一系列检查、评审点，实行分阶段的评审。由于产品的固有可靠性主要取决于设计，因此必须对规定的可靠性设计项目进行严格的评审，这是保证计划实现的重要管理环节，也是可靠性管理中的一项极为重要的制度。

可靠性设计评审的作用如下：

- 评价产品是否满足合同要求，是否符合设计规范及有关标准、准则。
- 发现和确定产品的薄弱环节、可靠性风险及其较高的区域，研究并提出改进意见。
- 对研制试验、检查程序和维修资源进行预先考虑。
- 检查和监督可靠性工作计划的全面实施。
- 检查设计更改，缩短研制周期，降低寿命周期费用。

3.5.2 评审组织及程序

评审是由一系列活动组成的审查过程，并按一定程序逐步开展和完成，大体分为5个阶段。

1. 准备

准备阶段的主要工作如下：



- 提出评审要求、目的、范围。
- 制订检查清单。清单中列出的项目是对可靠性有较大影响的若干重点；若干个根据设计、生产、使用经验提炼出来的准则或应注意的问题。
- 制订评审活动计划，规定时间、地点。
- 组成评审组，明确分工。评审组由负责设计项目的管理机构组织，一般由7~15人组成。组长职责是制订计划，明确审查小组分工，主持预审工作和评审会议，提出评审结论，签署设计评审报告。组长不应是被评审的设计项目的参加者。评审成员一般由主管设计师、非本系统的同行设计师、可靠性工程师、质量保证工程师、军事代表组成。
- 主管设计师汇集、提供评审所需的设计资料、试验数据，编写可靠性设计分析报告。可靠性设计分析报告的内容包括：设计依据、目标和达到的水平；设计的主要特点和改进方法；本阶段的可靠性分析、试验结果；对主要问题和薄弱环节的分析及对策；提交审查的设计、试验资料目录，以及有关的原始资料、结论；其他说明事项等。

2. 预审

预审由评审组成员根据设计按分工和职责进行评审检查。对发现的问题应记录在专门的表格中。评审组汇集、讨论预审中发现的问题，并反馈给主管设计师。

3. 正式会议评审

由主管设计师给出可靠性设计分析报告。评审组研究和讨论评审意见。

4. 编写评审报告

评审报告除应包括如前所述的各项内容外，还包括：评审组名单分工、设计目标及达到的水平、审查的项目及检查结果、重点问题审查结论、评审结论、不同意见备忘录、其他说明事项。

若评审报告认为必须进行重大改进或追补大量工作（如追加有关可靠性试验）时，则需要定期进行复审。

5. 追踪管理

对设计评审中提出的問題要制订对策，落实到人，限期解决。

3.5.3 可靠性评审

《可靠性维修性评审指南》对可靠性评审进行了详细的规定，是组织进行评审

工作的重要依据。

1. 评审的类型和评审点的设置

根据装备研制阶段、产品组成层次、评审的任务与范围的不同，一般可按下列类型选择和设置可靠性评审及评审点。

(1) 按研制阶段划分

- 论证阶段评审。
- 方案阶段评审。
- 工程研制阶段评审。
- 设计定型评审。
- 生产定型评审。

(2) 按产品组成层次划分

- 系统分级评审。
- 分系统分级评审。
- 系统级及其以下级别（设备、部件等）评审。

(3) 对转承制方和供应方的专题项目评审

根据研制工作的需要应对转承制方和供应方进行可靠性评审。

(4) 软件的可靠性评审

在系统研制和软件开发的全过程中应根据 GB 8566《计算机软件开发规范》、GJB 437《军用软件开发规范》、GJB 439《军用软件质量保证规范》的规定，进行软件的可靠性评审。

2. 产品研制各阶段的评审内容

(1) 论证阶段评审

其目的是评价所论证装备的可靠性定性与定量要求的科学性、可行性和是否满足装备的使用要求。评审结论为申报装备战术技术指标提供重要依据。

评审的主要内容是提出可靠性要求的依据、约束条件以及指标考核方案设想。

详细评审内容可参考《可靠性维修性评审指南》中的评审检查项，选择评审内容。

(2) 方案阶段评审

其目的是评审可靠性研制方案与技术途径的正确性、可行性、经济性和研制风

险。评审结论为申报装备的《研制任务书》和是否转入工程研制阶段提供重要依据。

评审的主要内容是评审可靠性工作计划的完整性与可行性、相应的保证措施，以及初步维修保障方案的合理性。

(3) 工程研制阶段评审

工程研制阶段的可靠性评审应根据实际情况具体安排，一般可进行两次评审，即初步设计评审和详细设计评审。

① 初步设计评审。

其目的是检查初步设计满足研制任务书对该阶段规定的可靠性要求的情况；检查可靠性工作计划的实施情况；找出可靠性方面存在的问题或薄弱环节，并提出改进建议。评审结果为是否转入详细设计提供重要依据。

评审的主要内容是评审在工程研制阶段各项可靠性工作是否满足要求。

② 详细设计评审。

其目的是检查详细设计是否满足任务书规定的本阶段可靠性要求；检查其工作实施情况；检查可靠性的薄弱环节是否得到改进或彻底解决。评审结论为是否转入设计定型阶段提供重要依据。

评审的主要内容是评审可靠性工作计划的实施情况、遗留问题的解决情况及可靠性已达到的水平。

(4) 设计定型评审

其目的是：评审可靠性验证结果与合同要求的符合性；验证中暴露的问题和故障分析处理的正确性与彻底性；维修保障的适应性。评审结论为能否通过设计定型提供重要依据。

评审的主要内容是评审装备可靠性是否满足《研制任务书》和合同要求。

(5) 生产定型评审

其目的是确认装备批生产中的必需资源和各种控制措施是否符合规定的可靠性要求。评审结论为装备能否转入批生产提供重要依据。

评审的主要内容是评审试生产的产品是否满足规定的可靠性要求，以及在批量生产条件下装备可靠性保证措施的有效性。

3. 评审的管理

可靠性评审的组织管理执行 GJB 1310A《设计评审》中第 5.3 条的规定, 评审程序执行 GJB 1310A 中第 5.2 条的规定, 并应同时考虑下列要求。

(1) 评审专业组的组成

评审专业组的组成人员应根据评审阶段和评审内容的不同, 而有所选择和区别。其中可靠性方面的技术专家应不少于 2/3, 并尽可能从相应的专业技术机构或评审委员会中选聘。

(2) 评审的准备工作

- 主管设计(论证)人员应认真准备设计(论证)工作报告及评审所需的其他文件, 提出《设计评审申请报告》。
- 有关业务主管部门负责组织拟定评审大纲和日程计划。

(3) 评审检查项目单

为了保证评审中对可靠性的有关问题都能给予适当的考虑, 评审主办单位应根据评审的需要并参照《可靠性维修性评审指南》中的附录 B、附录 C, 编制对可靠性工作情况和结果进行逐项核对与评价的检查清单。

(4) 评审后的工作

- 评审结束后, 评审组长应负责整理评审记录, 填写《评审报告》。
- 有关业务主管部门应对评审报告中提出的问题、解决措施和实施计划进行跟踪管理, 检查和监督其实施结果。
- 跟踪管理的结果应及时向有关部门反馈信息, 填写有关记录, 并作为下一次评审的输入信息。

(5) 评审文件管理

评审申请报告、评审记录、评审报告以及追踪管理的实施结果文件等, 应按规定传递、分发和归档。

3.5.4 软件可靠性设计评审

在软件开发的各阶段都要进行可靠性评审, 评审要求如下。

1. 软件需求分析评审

- 可靠性目标。



- 可靠性工作计划。
- 操作顺序及不可逆操作顺序的保障要求。
- 在功能降低使用的方式下，软件产品最低功能保证的规范。
- 选用或制订软件的可靠性设计准则及规范。

2. 概要设计评审

- 可靠性目标分配。
- 可靠性设计方案。
- 关键成分的时序、估计的运行时间、错误恢复。
- 测试的原理、要求、文件和工具。

3. 详细设计评审

- 各单元的可靠性目标。
- 各单元的可靠性设计（如容错设计）。
- 测试文件。
- 软件开发工具。

4. 软件验证和确认计划评审

- 软件可靠性的验证与确认方法。
- 软件可靠性测试（计划、规范、设施）。
- 验证与确认时所用的其他准则。

3.6 可靠性信息管理

可靠性信息是指有关装备的可靠性和费用等数据、报告与资料的总称。可靠性信息管理是对上述信息进行收集、传递、处理、储存和使用等的一系列活动，是可靠性管理的一项重要工作。

3.6.1 可靠性信息的分类

可靠性信息可以反映产品在不同寿命阶段的可靠性状况，以及各种有关因素对产品可靠性的影响和其变化规律。可靠性信息是进行可靠性设计、试验、管理、提高和保障产品可靠性的重要依据。

可靠性信息和所有的信息一样，按照不同的原则，从不同的角度，可以有不同的分类。

1. 按信息的来源分类

- 内部信息：由所管理的可靠性信息系统内部所产生的信息。
- 外部信息：由所管理的可靠性信息系统以外产生的与本系统可靠性工作密切相关的信息。

2. 按信息的作用分类

- 指令信息：是指与可靠性工作有关的来自上级的指令和规定，以及各领导层的各种决策目标和工作计划等。
- 反馈信息：是指在执行决策过程中所反映决策目标的正确性或偏离程度，以及用户对产品可靠性的反馈等信息。

3. 按问题的影响后果分类

- 严重异常的质量与可靠性信息：是指反映在产品的研制、生产、试验及使用过程中严重影响完成规定任务，导致（或可能导致）人或物发生重大损失的质量与可靠性信息。
- 一般异常的质量与可靠性信息：是指反映产品在研制、生产、试验及使用过程中不满足规定要求，但不致严重影响完成规定任务和不导致人或物发生重大损失的可靠性信息。
- 正常的质量与可靠性信息：是指反映产品在研制、生产、试验及使用中满足要求的质量与可靠性信息。

4. 按产品不同寿命周期中产生的信息分类

在产品的研制、生产和使用各阶段产生的可靠性信息等，称为 A 类信息。而 A 类信息经过汇总、分析、整理后，形成的在一定范围内具有指导意义的报告、手册等属于 B 类信息。

（1）A 类信息

① 产品在论证、研制、生产中的信息。

- 战术技术指标、研制任务书、合同中规定的质量与可靠性参数及指标。
- 可靠性工作计划、质量保证大纲及其评审报告。
- 可靠性指标的分配和预计结果。
- FMEA 和 FMECA 报告。
- 相关保障性的分析报告。
- 故障报告、分析、纠正措施及其效果。
- 关键件和重要件清单。



- 设计定型与生产定型时产品的质量与可靠性分析报告。
- 性能试验、环境试验、耐久性试验、可靠性试验、试车与试航等结果与分析报告。
- 可靠性增长计划及实施情况。
- 功能测试、包装、储存、运输及维修对产品质量与可靠性的影响。
- 对严重异常、一般异常的可靠性问题的分析、处理及其效果。
- 设计质量、工艺质量、产品质量评审结果及首件鉴定情况。
- 质量审核报告。
- 对关键件、重要件和关键工序的质量控制情况。
- 对不合格品的分析、纠正措施及其效果。
- 对外购件（含元器件、原材料）、外协件的质量复验报告。
- 产品的改进与改型情况。
- 产品验收及例行试验合格证。
- 质量成本分析报告。
- 其他有关信息。

② 装备使用、退役中的信息。

- 装备的使用情况。
- 故障报告、分析、纠正措施及其效果。
- 可靠性增长情况。
- 维修时间、间隔、次数、维修的等级、类别、维修方式、修理部位的难易程度、修理后使用的效果等。
- 装备的储存信息。
- 装备的检测信息。
- 装备的使用寿命信息。
- 对严重异常、一般异常的可靠性问题的分析、处理及其效果。
- 装备的改装及其效果。
- 装备在退役、报废时的可靠性状况。
- 综合保障情况、存在问题及分析，诸如：保障设备及设施、人员技能、训练器材、运输系统、各类技术资料等保障资源和综合保障工作的有关情况及存在问题。
- 装备质量与使用可靠性的综合分析报告。
- 承制单位的售后技术服务情况。
- 其他有关信息。

(2) B类信息

- 可靠性数据手册。
- 产品故障模式手册。
- 重大故障案例。
- 可靠性标准、规范。
- 可靠性技术文献。
- 可靠性试验报告。
- 可靠性研究报告及成果。
- 主要产品型号、规格、性能及生产厂家。
- 可靠性人才信息。

上述 A 类数据又分为实验室数据和现场使用数据。现场使用数据是可靠性数据的一个重要廉价来源,它比花费很大代价在实验室进行可靠性试验而得到的数据,更具有真实性和现实意义。

3.6.2 可靠性信息管理的工作内容

可靠性信息管理工作包括对信息的收集、加工处理、储存、反馈与交换,以及对信息利用情况的跟踪等内容。

1. 可靠性信息的收集

只有将分散的、随机产生的信息有目的地收集起来,并加以处理才能利用它为开展可靠性工作服务。从信息工作的全过程来看,信息收集是开展可靠性信息工作的起点,没有信息就无法进行信息的加工和应用。开展信息工作的关键和难点应在是否能做好信息的收集工作。

信息收集的程序如下。

(1) 确定信息收集的内容和来源

各级信息系统应具体确定信息收集的类别和内容。要逐项选择和落实它们的来源和渠道,对企业内部信息的收集,要按照信息流程图明确各级信息组织所应承担的任务,特别是要抓好各个信息源采集和记录信息的工作。对外部信息的收集,由于受多方面因素的制约,可控性差,困难也就比较大,因此,除了从上级和有关的信息组织可以获取信息外,要采取多种方式和手段间接收集有关的情报资料等,解决好信息的来源问题。



(2) 编制规范的信息收集表格

信息可以采用语言、文字、表格、磁带或软盘等不同的形式表达和记录。其中,信息表格是最基本的记录形式。因此,需要按照信息收集的类别和内容设计一系列的信息表格。

(3) 采集、审核和汇总信息

各信息源要按信息收集的计划和要求,选用所需的信息表格进行信息的采集和填写,并应有专人对所填信息表进行校核和审查。对遗漏的和有错误的信息,或者发现了新问题、新情况,则需要进行补充信息的收集。最后对信息进行汇总,并及时将信息按规定的信息流程提交或反馈给有关部门和信息组织。

2. 可靠性信息的加工处理

信息的加工处理主要是指对所收集到的、分散的原始信息,按照一定的程序和方法进行审查、筛选、分类、统计计算、分析的过程。

(1) 信息加工处理的一般程序和内容

虽然不同的信息管理层次对不同的信息加工的程序和内容各不相同,但一般对信息加工处理的程序及其内容应包括以下几点。

① 审查和筛选。

对收到的各类原始信息首先要进行再次的审查和筛选,审查信息的完整性和准确性,对不符合要求的信息,要求重新提供或加以剔除;对缺少的关键信息要进行补充;对有漏填的信息项而又难以补齐时,则应进行必要的技术处理。总之,要尽量减小信息的失真度,提高信息的完整性和准确性,使所需信息达到能够进行统计和分析的水平。

② 分类和排序。

将收集到的原始信息按规定的信息分类法进行分类,如分为:产品研制阶段的信息、用户反馈信息、严重异常的质量与可靠性信息、一般故障信息等。在分类的基础上,再根据信息的重要程度对信息进行排序,在实际工作中信息的排序就是提出那些严重异常的信息,或是与进行重大决策有关的信息,以便及时地予以提交和处理。

③ 统计和计算。

统计分析方法是处理可靠性信息最基本的方法。从大量数据的统计结果,往往就可以一目了然地看出产品可靠性的高低或发展趋势。数据不仅指的是数值,也包括任务完成与否、问题的严重程度等信息。统计、计算内容及分析参数则应按对信息的需求来选取。另外,在建立计算模型时,应注意要简单易行,便于在计算机上

数据的录入和处理,输出结果要易于为使用者所了解。

④ 分析与判断。

分析与判断是在上述工作的基础上,以决策目标、有关的指令和标准为依据,再加上人的经验和知识进行分析判断,并确定信息输出的内容、流向、方式和时间要求等。

⑤ 编写信息报告和输出信息。

将上述经过分析的信息定期或适时编制成信息报告(或资料),用以输出或储存信息。输出信息应尽量以图、表的形式表达,这样可以一目了然。

(2) 建立可靠性数据库

利用计算机分析、处理可靠性信息,为信息管理提供了有力的工具。必须做好可靠性数据库的建立和分析软件的编制工作。

数据库是按一定的结构方式存储在计算机硬盘和软盘中相关数据的集合。数据库技术可以将大量的数据独立于应用它的程序而存在,又具有最小的重复性和较高的可靠性,可以使数据具有共享性,即可以被不同用户的不同程序所使用,用户可以按需采取统一的控制方法,及时地对数据进行调用、查询和检索。

3. 可靠性信息的储存

信息经加工处理后,要分类储存,以便随时查询、使用。只有把信息科学地储存起来,才能在更广泛的范围内利用它,并有利于信息资源的再开发。

信息的储存有多种多样的方式,如文件、缩微胶片、计算机和声像设备等。过去传统的办法一般是采用文件的方式来储存信息。随着信息量的猛增以及计算机的广泛使用,信息的储存将逐渐被计算机数据库的方式所替代。应根据信息的利用价值、查询/检索要求,以及技术与经济条件来确定不同管理层次信息的储存方式。为了使以各种方式储存起来的信息能相互兼容和交流,应在信息分类的基础上,对信息进行科学的排序与编号,以便对储存的信息实施科学地管理。另外,还要按照信息的利用价值,对不同的信息确定不同的储存期限。

4. 可靠性信息的反馈、交换和传递

(1) 信息反馈

从闭环控制的角度看,信息反馈是指从受控系统向决策者输送信息,所以,信息反馈要及时、准确、完整和连续,并要求合理地设置信息反馈点、确定信息的流向和时限。

(2) 信息的交换

信息交换是指各企业、部门或各类信息组织之间相互提供彼此所需信息的过

程。信息交换是获取和利用信息的重要来源，是交换双方互通有无，实现信息资源共享，避免重复收集、重复试验，节约经费，争取时间，经济而有效地获取和利用信息的重要手段。

(3) 信息传递

信息只有经过传递才能发挥它的作用。可靠性信息的传递是实现可靠性信息闭环流动的的必要手段，因此，必须合理地选择信息传递的方式。

可靠性信息的传递是一种有意识、有目的的行动，为了提高“五位”信息系统工作的有效性，信息的传递要借助于一定的信息载体，如语言、文字、磁带、电波等，并通过一定的通道和方法，才能得以实现。因此，要根据信息量的多少、信息的重要程度和时限要求，以及技术、经济条件来合理地选取信息的通道和信息的传递方式。

3.7 故障报告、分析和纠正措施系统

3.7.1 概述

可靠性信息系统是指以装备（产品）为受控对象，以系统论和控制论为指导，由一定的组织、人员、设备和软件组成的，按照规定的程序和要求，从事可靠性信息工作，以支持和控制可靠性工程活动有效运行的系统。可靠性信息所具有的特征决定了它是一个多层次、多环节、多专业的相互关联的复杂系统。

建立故障报告、分析和纠正措施系统（FRACAS）的目的是及时报告产品的故障，分析故障原因，制订和实施有效的纠正措施，以防止故障再现，改善其可靠性和维修性。它是促进产品可靠性增长、提高产品质量的重要手段。

可靠性管理是通过制订目标、组织实施、督促检查，根据检查取得的信息及时给出处理决策以控制和提高产品可靠性，完成管理上的一个个循环。要实现上述目的，首先必须使可靠性信息流通形成闭环。在研制过程中，可靠性信息闭环管理的有效方法是建立 FRACAS。一切可靠性活动都是围绕故障展开的，都是为了防止、消除和控制故障的发生，所以，对研制、制造、试验过程中出现的故障，一定要充分利用故障信息去分析、评估和改进产品的可靠性。FRACAS 应按规定的程序进行，以使可靠性信息形成闭环。

该系统主要适应于产品的研制阶段，也适应于生产阶段和使用阶段。因为在研制阶段采取纠正措施时选择的灵活性最大，最易于实施，效果也最明显。在生产和

使用阶段也可以采取纠正措施，但将会受到很大的限制。因此，承制单位应及早建立该系统。

FRACAS 的主要任务，就是对可靠性信息系统的建立和运行的管理，其主要的工作内容如下：

- 制定必要的规章制度和有关规定。为保证可靠性信息系统正常的运行，要制定信息工作的政策、法规、标准和规范，以及信息组织的管理章程和有关的工作细则等，使信息、工作制度化和规范化。
- 进行信息工作技术的基础建设。为开展可靠性工作的需要，应进行必要的技术设计，制订规范化的信息表格和信息代码系统，编制配套的计算机数据库和分析软件，开展信息分析处理、传递和应用等信息技术和方法的研究工作。
- 进行信息需求的分析。对信息的实际需求是开展信息工作的依据。各级信息组织和信息用户都应进行信息需求分析，明确信息收集的内容和工作重点，以便节约人力和财力，提高信息工作的实际效益。
- 实施信息的闭环管理。对信息实施闭环管理是开展可靠性信息工作的基本原则。信息的闭环管理有两层含义：一是信息流程要闭环；二是信息系统要与有关的工程系统相结合，不断地利用信息解决实际问题，形成闭环控制。为此要依据对信息的需求，对信息流程的每个环节进行有效管理，并对信息的应用效果进行不间断的跟踪。
- 信息员的技术培训。信息工作人员的素质是搞好信息工作的关键。要有计划地开展技术培训工作，建立一支从事可靠性信息工作的专业队伍。
- 考核和评定信息系统的有效性。对信息系统应进行定期的考核和评估，以提高信息系统运行的有效性。

3.7.2 FRACAS 系统的建立

1. 制订故障报告闭环系统的计划

该计划应包括：故障报告、故障分析和纠正措施反馈的程序；故障信息传递和故障件处理的流程图；故障分析和纠正措施实施状态的跟踪与监控的程序；故障审查组织的职权和其办事机构的职责等内容。计划应得到订购方的认可。

计划应有如何实现故障报告闭环系统的初步方案，应有一套用来控制故障报告、故障分析和纠正措施反馈的程序；应有反映故障发生、分析和纠正整个过程的流程图，如图 3-4 所示给出了一个故障报告闭环系统工作流程图的示例；应有

故障信息和故障件在承制方内部流通的程序；应有故障报告、故障分析和纠正措施报告的格式，表格的形式应考虑填写简便，有利于故障信息的追溯和便于所需信息的提取。

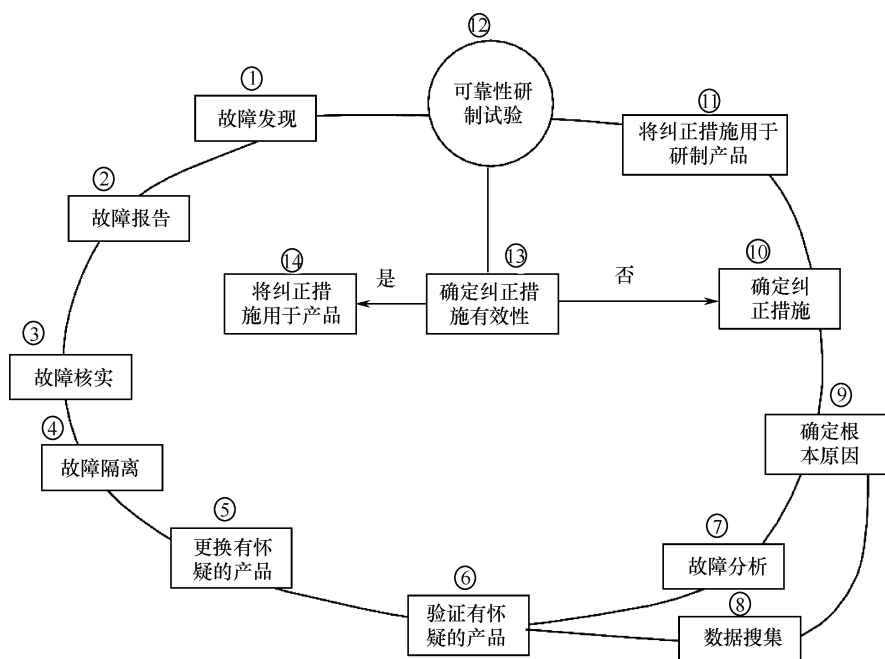


图 3-4 故障报告闭环系统工作流程图

2. 建立 FRACAS 系统

故障报告闭环系统应由承制（及转承制）方尽早建立，并在订购（使用）方的协同下加以实现。该系统应保证对合同规定层次的产品在研制阶段和生产阶段所发生的故障进行及时报告、分析和纠正。转承制方应将所承制的产品在研制阶段以及生产阶段发生的故障信息汇总到承制方的信息系统中，以利于跟踪故障和纳入承制方相应的故障文件。承制方应利用现有的信息收集、分析和纠正系统，只有该系统不能满足订购方的要求时，才进行修改。

订购（使用）方应将产品的故障信息及时反馈给故障报告闭环系统。

故障报告闭环系统应尽早地建立和运用，因为在设计进展期间纠正措施的选择方案时，其灵活性最大，根据已知的故障原因，可以进行较大的设计更改，在生产阶段或使用阶段虽然也能采取纠正措施，但方案选择受到限制，实施也更困难。故障原因弄清得愈早，切实的纠正措施采取得愈及时，承制方与使用方取得的收益就愈快、愈大。对于那些需要做较多工作的故障，及早采取纠正措施还有

利于提前摸清什么措施更为有效。对可能发生的故障，应进行早期调查分析，采取纠正措施，避免使问题积压起来，或使若干早可纠正的缺陷，留到现场服务中去解决。

3. FRACAS 的故障审查组织

为了审查重大故障、故障趋势及纠正措施，承制（转承制）方根据其机构设置的具体情况，可成立专门的故障审查组织，亦可由能完成故障审查任务的机构负责此项工作。故障审查机构与质量保证部门的工作应协调一致。

（1）故障审查组织的组成

故障审查组织由承制（转承制）方的设计、生产、可靠性、维修性、安全性和质量保证等方面的代表组成，订购方可派代表参加。故障审查组织的办事机构由质量保证部门或其他技术部门承担。

（2）故障审查组织的职权

- 定期召开会议，审查产品研制阶段以及生产阶段出现的故障信息，包括转承制方和订购方反馈的故障信息，分析、评审有关产品的故障趋势和纠正措施的实施效果。
- 对重大的故障、频繁出现的故障，以及可靠性关键件和重要件的故障应及时开会分析，提出纠正意见。
- 有权要求转承制方对所承制的产品进行故障调查和分析，并评审其纠正措施。
- 对悬而未决的问题有权追查，并提出其处理意见，必要时向有关领导部门报告。

（3）故障审查组织办事机构的职责

- 负责处理故障审查组织的日常事务工作。
- 负责对合同规定层次产品的故障报告进行收集、分类，并按规定程序传递及组织归档。
- 负责检查故障分析和纠正措施的进展情况。
- 负责提出故障趋势的意见。
- 负责提供故障审查组织召开审查会议需要的有关资料，并对会议纪要进行归档。

4. 故障文件的编制

对所有故障（故障原因）的调查和分析、采取的纠正措施及效果、故障审查活

动等均应记录并保存，将这些记录编制成有统一编号的故障文件，以便检索、查阅和订购方在合同期内审查。故障文件除故障报告、故障分析报告和纠正措施实施报告外，还应编制故障概要或状态报告。

5. 与其他工作的关系

若质量、可靠性、维修性、安全性、试验和综合后勤保障等计划都要求运用故障报告闭环系统时，此项工作应综合考虑，统筹协调。下面以 FRACAS 与故障模式、影响及危害性分析的关系为例，说明两者之间应如何协调。

故障模式、影响及危害性分析是根据可利用的资料，利用工程简图和任务剖面图的要求来发现设计中潜在的薄弱环节，对可能出现的故障模式，确定其对系统（人员）安全、系统性能、可靠性、维修性等产生的影响和危害。对每种故障模式，通常用故障影响的严重程度以及发生的频度估计危害程度。根据危害程度采取适当的措施，使故障及其后果最大限度地减少或完全消除。

故障报告闭环系统是确保合同规定产品层次的故障都能得到报告，进行分析后采取有效的纠正措施，防止或减少同类故障的再次发生。故障模式、影响及危害性分析作为综合的信息来源，为故障报告闭环系统评审实际发生的故障提供了依据。而故障报告闭环系统又可为评价故障模式、影响及危害度分析的完整性和准确性提供了资料。这两种工作的效果应当具有一致性，如存在重大差别，就要重新评价产品可靠性设计的依据和故障准则。尽管两者是分别构思和独立完成的，但两者配合应用，其效果就更加明显。

3.7.3 FRACAS 的运行

FRACAS 运行的程序如图 3-5 所示。

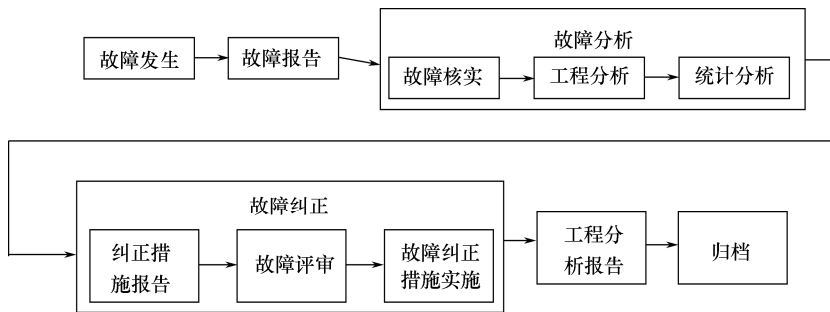


图 3-5 FRACAS 程序图

整个运行程序围绕故障展开，历经故障发生、报告、核实、分析、纠正和闭环管理、归档等过程。

1. 故障报告

故障信息首先通过故障报告系统来建立。在研制和生产、试验过程中发生的所有硬件和软件故障，均应按规定的格式和要求进行记录，在规定的时间内向规定的管理级别进行报告。

合同规定层次产品所发生的故障都应及时报告。故障报告内容应包括：识别故障件的信息、故障现象、试验条件、机内检测（BIT）指示、发生故障的产品工作时间、故障观测者、故障发生时机，以及观测故障时的环境条件等。故障报告内容应准确填写。

2. 故障核实

对报告的故障内容都应按发生故障时的实际情况进行核实。故障核实可通过重现故障模式或依靠故障证据（漏泄残余、损坏的硬件和机内检测指示等）来完成。对缺乏证据的情况应给予说明。

3. 故障分析

对报告的故障应进行必要的分析，以确定故障原因。故障报告闭环系统应对故障调查和分析提供有关的文件资料。故障分析应从需要的硬件或软件产品层次进行。根据具体情况可采用试验、分解、X 射线、显微镜分析和应用研究等方法，进行故障调查和分析。

故障分析的目的就是确定故障原因和机理，为制订纠正措施提供依据。

故障分析首先应由专业人员审查故障信息，然后制订分析流程图，确定跟踪和监控故障分析工作的方法，以保证按时完成分析工作。

故障分析应按下述程序进行：

- 故障调查与核实。应调查和核实故障产品的工作状态和环境情况，故障现象和特征，试验程序、方法和设备是否包含导致故障发生的因素，试验人员操作的可靠性。必要时，应做故障复现试验，以证实故障状态的各种数据。
- 故障工程分析。在故障核实后，可对故障产品进行测试、试验、观察和分析，确定故障部位，并弄清故障产生的机理。
- 故障统计分析。收集同类产品的生产数量、试验和使用时间、已产生的故障数，估算该类故障出现的频率。

故障分析可采用工程或实验室的分析方法，简述如下：

- 设计师与可靠性工程师之间的技术讨论。
- 进行故障环境的调查。



- 进行分解、X射线和显微镜分析等。
- 对某些特殊情况，采用实验室分析方法。
- 可与同类故障信息进行比较分析。
- 其他分析。

4. 纠正措施

故障原因确定以后，应由责任单位制订纠正措施，编制相应的文件，予以实施，防止或减少同类故障的再次发生。纠正措施应按工程更改程序的有关规定进行。

分析结果应反馈给专业技术人员，使他们可以采取适当的措施来解决或缓解问题，例如制造中实行新的控制方法、更改设计、更改工艺或材料、更换一个满足使用要求的较好元器件等。实行纠正措施以后应加以监视，保证纠正措施能排除故障，而且不产生新的问题。

通过故障分析查明故障原因和责任，以便有针对性地采取纠正措施。纠正措施要经过分析、计算和必要的试验验证，并经评审通过后，方可付诸实施。

故障纠正活动完成后，应编写故障分析报告，汇集故障分析和纠正过程中形成的各种数据和资料，并立案归档。

5. 故障闭环管理

对报告的每个故障应根据本标准的要求及时地予以分析，采取纠正措施，使其取得效果，并使难处理的或尚未解决的故障积压减少到最低程度。在纠正措施实施并证实有效或不采取纠正措施的故障说明理由以后，可以认为故障报告的工作已经完成。对悬而未决的问题应当及时审查，确定其终止日期，以确保及时结束故障报告工作。对未能采取纠正措施的情况，经故障审查组织核准后作为遗留问题，立案备查。

6. 故障件的识别和控制

对所有的故障件应给出明显标记以便于识别和控制，确保按要求进行处置。为便于进行故障调查和分析，必要时应对现场加以保护。故障调查和分析完成后，典型的、重要的故障件应妥善保管。

7. 故障信息管理

故障信息应保证完整性和准确性。对所有报告的故障信息应统一管理和保存，保存时可采用文字档案和数据库的方式。

参 考 文 献

- [1] GJB 450A-2004. 装备可靠性工作通用要求.
- [2] GJB 841-1990. 故障报告、分析和纠正措施系统.
- [3] GJB 1686A-2005. 装备质量信息管理通用要求.
- [4] GJB/Z 77-1995. 可靠性增长管理手册.
- [5] XKG/D01-2009. 型号 RMS 管理指南. 北京: 国防科技工业可靠性工程技术研究中心, 2009.
- [6] XKG/D08-2009. 型号质量与可靠性信息管理指南. 北京: 国防科技工业可靠性工程技术研究中心, 2009.
- [7] 张增照. 以可靠性为中心的质量设计、分析和控制. 北京: 电子工业出版社, 2010.
- [8] 谢千跃, 宁书存, 等. 可靠性·维修性·保障性·测试性·安全性概论. 北京: 国防工业出版社, 2012.
- [9] 秦英孝, 张耀文, 等. 可靠性·维修性·保障性管理. 北京: 国防工业出版社, 2003.
- [10] 孙青, 庄亦琪, 等. 电子元器件可靠性工程. 北京: 电子工业出版社, 2002.
- [11] 罗新华, 高俊峰, 等. 装备研制过程质量监督. 北京: 国防工业出版社, 2013.

第4章

可靠性要求

4.1 确定可靠性要求的重要性

可靠性要求是产品或系统可靠性工作要达到的目标，是进行产品可靠性设计、分析、试验和验收的依据。科学、合理地确定可靠性要求是一项重要而复杂的系统工程，也是可靠性工作的首要任务。

可靠性是衡量产品质量优劣的重要指标，它体现了使用者对产品可靠性的需求，同时也反映出研制者具备的可靠性能力水平。如果可靠性要求偏低，将影响产品的使用效果；可靠性指标过高，则可望而不可即，无疑会增加产品的研制难度、周期、成本，甚至导致产品研制无法达到预期目标，乃至失败，因此，合理地确定可靠性要求是产品论证中要解决的重要问题。

可靠性是装备的重要质量特性，并与成功概率和故障频率密切相关，对产品的适用性和使用效能具有重要影响。从基本可靠性出发，它与装备的维修所需的保障资源密切相关，是适用性范畴内的重要特性之一，直接影响装备的适用性；从任务可靠性出发，它与装备完成任务的程度有关，并直接影响装备使用效能。

可靠性也是影响装备寿命周期费用的重要因素。如何降低产品的寿命周期费用，尤其是使用与保障费用，已成为产品决策的重要因素和新产品研制的重要目标之一。为了降低新研制产品的寿命周期费用，必须将可靠性与其他相关的通用质量特性及技术性能进行权衡分析，再合理确定可靠性要求。

4.2 可靠性要求的表述形式

归纳起来，可靠性要求的表述形式有如下3种。

- 明确表述。用户（客户）在合同或技术要求文件中明确描述了可靠性要求及

其验证方法。例如,规定了产品的使用寿命、可靠度、平均故障间隔时间和使用环境条件,以及通过何种方法(如鉴定和验收试验、分析评估、演示、使用验证等)来验证这些要求。大部分军用装备的研制和民品合同研制项目都采用这种形式。在这种情况下,可靠性要求是产品合格验收的重要依据。

- 含蓄表述。用户在合同或技术要求中没有明确描述具体的量化可靠性要求,但描述了使客户满意的达到指定水平可靠性的产品相关特性或使用要求,例如:寿命周期费用、保障费用,以及维修人力、保证条款等与产品使用相关的要求。在这种情况下,需要根据所描述的产品特性要求或使用要求导出可靠性要求,此过程基于已知的或假设的特性关系进行,经常采取权衡分析方法。
- 没有表述。这种情况下,并非产品没有可靠性要求,而是对要求没有具体的表述。商用货架产品大多属于这种情况。通常情况下,供应商根据市场需求预先考虑其产品投放市场后对可靠性的要求和定位,然后反馈给产品承制方。承制方有时可能有相似产品或竞争产品可靠性的数据,也可能没有。在这种情况下,经常采用市场(需求)调查、质量功能展开、相似产品法(如存在相似产品)等方法。

4.3

与可靠性要求相关的若干概念和参数

有关可靠性要求的概念,主要涉及可靠性定量要求参数和使用剖面等,部分已在前面的章节中介绍过,为方便读者理解,这里进一步总结归纳如下。

- 可靠性参数:描述可靠性的特征量,或者是对可靠性的一种度量,对于武器装备而言,通常将其分为两大类,即可靠性使用参数和可靠性合同参数,由于需求不同,在不同场合将选择不同的使用参数和合同参数。
- 可靠性使用参数:直接与装备(战备)完好性、任务成功性、维修人力费用和保障资源费用有关的一种可靠性度量。使用可靠性参数示例见表4-1。
- 可靠性合同参数:是指在合同中表述订购方可靠性要求的,并且是承制方在研制和生产过程中可以控制的参数。常用的合同参数见表4-2。
- 可靠性指标:对可靠性参数的度量值为可靠性指标,可靠性指标随其度量的参数又可分为使用指标和合同指标,使用指标(使用值)包括门限值与目标值,合同指标(合同值)包括最低可接受值与规定值。
- 门限值:订购方(军方)可以接受的最低限度的使用值,是确定合同指标最低可接受值的依据。
- 目标值:高于门限值且在使用中期望达到的量值,是确定合同指标规定值的依据。目标值和门限值之间是进行权衡(技术、经济、进度)的空间。

- 最低可接受值：合同或研制总要求中规定的，装备必须达到的合同指标，是设计定型时验证的依据。
- 规定值：高于最低可接受值，是装备（产品）设计的依据，一般产品应按高于规定值进行设计。
- 寿命剖面：产品从交付到寿命终结或退出使用的阶段内所经历的全部事件和环境的时序描述。寿命剖面应反映装备在整个生命周期中全部典型的经历，它可能包括一个或几个任务剖面。寿命剖面是订购方根据新研制装备的任务需求、使用方案和使用要求等确立的，为新装备的论证、研制、生产、试验、使用与维修保障提供依据，寿命剖面是确定、验证、评价基本可靠性要求的依据。
- 任务剖面：产品在完成规定任务时间内所经历的事件和环境的时序描述。它应包括任务成功或严重故障（原称致命性故障）的判别准则。任务剖面是确定和验证、评价任务可靠性要求的依据。

表 4-1 可靠性使用参数示例

使用特性	可靠性使用参数示例	
战备完好性	A_O （平时）	平均不能工作事件间隔时间（MTBDE） MTBDE=寿命单位总数/不能工作的事件总数
	SGR（战时）	
任务成功性	平均严重故障间隔时间（MTBCF） MTBCF=任务总时间/严重故障总数	
维修人力和保障资源费用	平均维修间隔时间（MTBM） MTBM=寿命单位总数/（（计划+非计划）维修事件总数）	
	平均拆卸间隔时间（MTBR） MTBR=寿命单位总数/拆下其组成部分的总数	
注： A_O 为使用可用度，SGR为出动架次率		

表 4-2 常用的可靠性合同（设计）参数

产品层次	产品的工作特征		
	连续或间歇工作（可修复）	连续或间歇工作（不可修复）	一次性使用
系统	$R(t)$ 或 MTBF、MTBCF	$R(t)$ 或 MTTF	$P(S)$ 或 $P(F)$
分系统 设备	$R(t)$ 或 MTBF、MTBCF	$R(t)$ 或 λ	$P(S)$ 或 $P(F)$
组件 零件	λ	λ	$P(F)$

注： $R(t)$ ：可靠度；MTBF：平均故障间隔时间； $P(S)$ ：成功概率；MTTF：平均故障前时间； $P(F)$ ：故障概率；MTBCF：平均严重故障间隔时间； λ ：故障率

4.4 可靠性要求

可靠性要求分为两大类：第一类是定性要求，即用一种非量化的形式限制产品设计和评价，从而保证产品的可靠性；第二类是定量要求，即规定产品的可靠性参数、指标和相应的验证方法，用定量方法进行设计分析，用增长或验证方法进行可靠性验证，从而保证产品的可靠性。

4.4.1 可靠性定性要求

可靠性定性要求是与产品可靠性定量要求同时提出的对产品设计、工艺、软件等方面的非量化要求，例如采用成熟技术、简化、冗余和模块化等设计要求，有关采用元器件、原材料、降额、热设计和健壮设计等方面的要求（见表 4-3）。可靠性定性和定量要求应该是相辅相成的。定量要求是必需的，是验证的依据，定性要求是达到定量要求的必要条件和补充，是可靠性要求不可或缺的部分。对一个具体装备的可靠性定性要求应该是上述原则性定性要求的具体化。

表 4-3 主要的可靠性定性要求

序 号	要求类别	目 的
1	制订可靠性设计准则	将可靠性要求及使用中的约束条件转换为设计条件，给设计人员规定了专门的技术要求和设计细则，以提高产品可靠性
2	简化设计	降低产品的复杂度，以提高其基本可靠性
3	余度设计	通过两种或两种以上技术途径以实现规定的功能，提高产品的任务可靠性和安全性
4	降额设计	降低元器件、零部件的故障率，提高基本可靠性、任务可靠性和安全性
5	元器件、零部件的选择与控制	对电子元器件、机械零部件进行正确的选择与控制，提高产品可靠性，降低保障费用
6	确定关键件和重要件	把有限的资源用于提高关键产品的可靠性
7	环境防护设计	使用能减轻环境作用（或影响）的设计方案和材料，或提出能改变环境的方案，或把环境应力控制在可接受的范围内
8	热设计	通过元器件的选择、电路设计、结构布局设计，减少温度对产品可靠性的影响，使产品能在较宽的温度范围内可靠工作
9	包装、装卸、运输、储存设计等	通过对产品在包装、装卸、运输、储存期间性能变化情况的分析，确定应采取的保护措施，从而提高其可靠性

注意，产品可靠性定性要求应考虑如下方面：

- 不易用定量指标来描述的可靠性要求，如紧固件锁紧时应牢固、可靠等

要求。

- 有关使用操作方面的可靠性要求，如操纵件与人的因素有关的要求。
- 对危及或可能危及产品安全的故障提出的保护或预防措施等要求。
- 软件可靠性要求一般应高于所嵌入硬件的可靠性要求。

4.4.2 可靠性定量要求

GJB 450A 将可靠性定量要求分为 4 类，如表 4-4 所示。其中，基本可靠性要求和任务可靠性要求又可分为反映使用要求的可靠性使用要求（用使用参数和使用值描述），以及用于产品设计和质量监控的可靠性合同要求（用合同参数和合同值描述）。

表 4-4 可靠性定量要求分类及示例

定量要求分类	定量要求示例
基本可靠性	平均维修间隔时间（MTBM）（使用要求） 平均故障间隔时间（MTBF）（合同要求）
任务可靠性	平均严重故障间隔时间（MTBCF） 任务可靠度（ $R(t)$ ） （使用需求或合同要求）
储存可靠性	储存可靠度
寿命（耐久性）	首翻期、翻修间隔期限、使用寿命、储存寿命

1. 关于可靠性使用要求和可靠性合同要求

使用可靠性是产品在实际使用条件下所表现出的可靠性，它反映了产品设计、制造、安装、使用、维修、环境等因素的综合影响。固有可靠性是通过设计和制造赋予产品的，并在理想的使用和保障条件下所呈现的可靠性。即便是同一产品，它的实际使用保障条件和合同规定的条件是不同的，使用可靠性和固有可靠性的故障判据也是不同的，固有可靠性只能考虑那些与产品设计和制造有关的故障（关联故障），因此同一产品所表现出的使用可靠性水平和固有可靠性水平是不同的，而且固有可靠性水平是高于使用可靠性水平的。装备的可靠性要求首先是军方根据使用要求提出的可靠性使用要求，即在实际使用保障条件下要求装备达到的可靠性水平，可靠性使用要求中有些因素是不能直接用于产品设计的，必须剔除那些非设计和制造因素，转换为合同要求，这就是通常所说的，需要把可靠性使用要求转换为可靠性合同要求。

可靠性使用参数是直接 with 战备完好性、任务成功、维修人力费用和保障资源费用有关的一种可靠性度量。可靠性合同参数是在合同中表达订购方可靠性要求的，并且是承制方在研制和生产过程中可以控制的一种可靠性度量。从原则上讲，描述可靠性使用要求一般应该用可靠性使用参数及其量值来表达，使用参数便于在实际

的使用条件下度量, 可靠性合同要求用可靠性合同参数及其量值来描述, 可以在合同规定的条件下验证。从使用要求转换为合同要求, 客观上就存在参数和量值的转换问题, 但其实质上是由环境因素和故障判据不同而引起的差别, 即便使用参数与合同参数采用了相同的参数, 但由于两者内涵上的区别, 在量值上也是不同的。

2. 用户的使用要求是导出可靠性使用要求的依据

系统战备完好性、任务成功、维修人力费用和保障资源费用等是与可靠性密切相关的用户使用要求。要根据这些使用要求导出装备的可靠性使用要求, 或者说装备可靠性要求与相关特性要求一起应能满足上述用户的使用要求。对于基本可靠性要求, 理想的情况是建立某种使用要求与可靠性的关系式, 以便导出可靠性要求, 例如使用要求是使用可用度 (A_O), 则可利用下式:

$$A_O = \frac{MTBM}{MTBM + MDT} \times 100\% \quad (4-1)$$

式中: A_O ——使用可用度;

MTBM——平均维修间隔时间 (可靠性使用参数);

MDT ——平均不能工作时间。

如果根据部队类似装备的实际经验, 假设 $MDT=12.5h$, 要求 $A_O=80\%$, 则可导出 $MTBM=50h$ (基本可靠性)。

对于任务可靠性, 可以利用任务可靠性与任务成功性的如下关系式导出任务可靠性要求:

$$D=R_M + (1-R_M) M_O$$

式中: D ——任务成功性参数;

R_M ——给定任务剖面下的任务可靠度;

M_O ——给定任务剖面下的修复概率。

当给定 M_O 时, 即可根据要求的任务成功性 D 导出任务可靠度, 当任务期间不能维修时, 任务成功性等于任务可靠性。

一些可靠性参数可从装备的使用要求直接得出。例如, 对于通信系统而言, 战时必须保证其能正常通信。按一个合成集团军遂行一次战役任务时间 7 天考虑, 由此可得出通信系统的平均不能工作事件间隔时间 (MTBDE) 应不小于 168 小时。

3. 使用可靠性要求转换为设计 (合同) 可靠性要求

将可靠性使用要求转换为可靠性设计要求的目的是为承制方 (设计者、生产

者)规定通过设计和生产可以控制的可靠性要求,达到了可靠性设计要求,意味着可靠性使用要求也就“自动”满足了,因此,这种“转换”就显得非常重要,如果转换不适当,“设计要求”达到了,而“使用要求”却不能满足,或者说“设计要求”过高了,增加了研制的成本。总之,在确定可靠性要求的过程中,“转换”是个很关键的问题。“转换”通常可通过两种途径来实现:一是建立使用可靠性和设计可靠性之间的关系模型,确定影响转换的各种因素,然后通过收集使用、维修和设计数据,确定存在关系数并验证这些模型;另一种做法是根据工程经验采用简单的“K 系数”,建立使用可靠性与设计可靠性的关系。此外,使用参数指标转换为合同参数指标有两种情形:一种是同名参数的转换;另一种是异名参数的转换。同名参数的转换只是转换了指标要求的量值,异名参数的转换不仅改变了指标要求的量值,也改变了指标的含义。

不论是哪种情形的转换,一般都可用线性和非线性转换模型。

$$Y = a + bX \quad (4-2)$$

$$Y = bX^a \quad (4-3)$$

式中, Y 表示合同指标; X 表示使用指标; a, b 表示系统的复杂性、使用环境、保障条件和指挥管理水平等因素的转换系数。

例如,某系统将参数可用度 A_o 转换为合同参数可用度 A_i 的转换模型是:

$$A_i = aA_o \quad (4-4)$$

只要在研制中保证 A_i , 就可在使用中保证 A_o , $a = 1.25$ 。

又如,罗姆实验室建立一种飞机通信系统的转换模型,将平均维修间隔时间 MTBM 转换为平均故障间隔时间 MTBF, 公式如下:

$$MTBF_p = \left[\frac{MTBM}{r_E r_M} \right]^{1.45} \quad (4-5)$$

式中: $MTBF_p$ ——失效率预计值(设计参数);

MTBM ——平均维修间隔时间(使用参数);

r_E ——环境因子,设备在载人区时取 1.41,在非载人区时取 1.55;

r_M ——任务剖面因子,具体计算公式如下:

$$r_M = \left[\frac{\text{每次任务设备的通断次数}}{\text{任务时间}} \right]^{-0.57} \quad (4-6)$$

当运输机上雷达的使用可靠性 $MTBM=500h$, 任务平均时间为 3h, 雷达安装在非载人区,并在任务期间一直处于工作状态,利用式(4-5)可解得 $MTBF_p=1751h$ 。

4.5 确定可靠性要求的一般原则和实施要点

确定可靠性要求时一般应遵循如下原则。

1. 满足使用要求原则

提出可靠性要求时，应从产品的使用需求出发，使最终产品满足使用要求。

产品或装备的使用要求是具体新研制或改进产品使用方案，以及详细性能和能力的说明。使用要求中的装备（战备）完好性、任务成功性，以及有关使用保障能力和费用等是导出装备可靠性要求的依据。

装备的基本可靠性要求由装备（战备）完好性要求导出；装备的任务可靠性要求源于任务成功性要求；装备的储存可靠性要求和寿命要求应考虑装备的设计方案、使用方案、维修保障能力及费用等因素。

2. 可行性原则

可靠性要求必须是现实可行的，因此，论证可靠性时应进行可行性分析，包括科学性、先进性、技术与经济方面的可行性分析。

可靠性要求的确定要有科学的依据，这些依据包括如下几项。

- 使用需求。产品使用需求是确定可靠性要求的主要依据，它包括产品要求完成的任务或执行的功能、任务持续时间及次数、利用率、使用环境和使用寿命等。
- 相似产品的可靠性水平。相似产品指的是与拟研制的产品在功能、技术水平、复杂程度、使用环境、使用和保障方案等方面相似的在用产品，其现场使用数据是确定新研产品指标的主要依据之一。相似装备的可靠性水平是初定可靠性要求的重要参考。相似装备的可靠性水平是新研装备初定可靠性要求的参考，这里有两层含义，一是尽可能选择类似装备惯用的可靠性参数，这样有利于该军种装备可靠性水平的评价和比较；二是收集分析相似装备的使用数据，参考类似装备的可靠性水平和问题，依据新研装备的使用要求初定可靠性要求。
- 预期采用的新技术可能使产品达到的可靠性水平。这是确定可靠性要求的重要依据。新研产品一般会采用新的技术和方法，使其可靠性水平比现有类似产品有所提高，从而可能达到新的可靠性水平。
- 产品的研制经费、周期、预期的使用和保障方案等约束条件。研制费用和进度要求对产品的可靠性要求会产生较大的影响。不同的产品使用方案（要求）对产品的可靠性要求也不同。例如，部署在沿海及亚热带地区的产品，



在确定其可靠性要求时，必须充分考虑盐雾及潮湿对产品结构及设备产生的腐蚀影响。维修和保障方案（策略）对产品的可靠性要求也会产生影响。相对而言，保障方案中维修周期长或备件量少且价格昂贵的部分，其可靠性要求应定得高一些。

3. 可验证原则

可靠性要求应是可验证的。提出的可靠性参数数量应尽量少，定量要求应有明确的定义，有明确的验证时机、内容、条件和方法；定性要求应以明确的语言表达出各项要求，可评估、可检查，并有检查清单和检查方法。

例如，平均维修间隔时间（MTBM）是使用可靠性参数，等于寿命单位总数与总数计划和非计划维修事件之比。首先，必须明确它是一个在产品使用中度量的参数，定义的同时必须规定统计的时间段和采用的时间单位，统计计划和非计划维修事件的准则等。又如 MTBF 这个参数，当用于使用条件或合同环境时，规定的故障判据应该是不同的，所以在选用这个参数时，必须有明确的故障统计准则。可靠性定量要求只有可度量，才是可验证的。

4. 协调性原则

提出的可靠性要求应完整，相互协调配合，并确保最终提出的可靠性要求与产品设计方案、使用方案相协调。

装备的可靠性、维修性对于相同的固有可用度而言是一对互补的特性，即可靠性提高一些，维修性可以低一些，可靠性差一些，可用提高维修性来补偿。好的测试性，能够提高维修性水平，对于相同的使用可用度，固有可用度与保障系统的能力又是一对互补的特性。由此不难看出，可靠性仅是影响战备完好性、任务成功性的重要因素之一，在确定可靠性要求时，必须充分协调这些相关的要求，如维修性、测试性、保障系统能力等，以最佳的匹配满足战备完好性、任务成功性等使用要求，这就是在 GJB 1909A 中规定的，应整体性地形成可靠性、维修性、保障性要求。

确定可靠性要求是一个反复迭代的过程。确定可靠性要求，需要经历一个反复权衡、协调的过程，即初定到确定的过程。对初定的可靠性要求和其他相关要求进行技术可行性、费用等权衡分析工作，需要时应对初定的可靠性和其他相关要求进行调整，以最佳的匹配满足使用要求。可靠性要求与设计方案密切相关，当设计方案改变时必须对可靠性要求进行可行性分析。

任务可靠性和基本可靠性要求是为分别满足任务成功性和战备完好性而确定的，当为满足任务成功性而要求提高任务可靠性（冗余、备份）时，会引起基本可靠性的下降，为此，在确定可靠性要求的过程中，应紧密结合装备的设计方案，同时满足任务可靠性和基本可靠性要求。

确定可靠性要求的要点和注意事项如下：

① 产品可靠性要求与产品使用功能要求一样重要,因此产品立项报告和研制开发策划均应包括可靠性要求论证的内容。

② 产品可靠性论证应根据产品满足顾客要求的能力,以达到顾客满意为出发点,通过对产品的结构分析、系统分析、功能分析提出并评价产品可靠性要求。

③ 在确定可靠性要求时,应通过权衡分析来实现各 RMS 要求之间的相互协调,包括 RMS 要求与性能、费用之间的协调;可靠性(RMS)要求之间、RMS 要求与安全性要求之间、基本可靠性与任务可靠性要求之间,以及合同要求与使用要求之间的协调。主要考虑如下方面:

- 可靠性要求与性能、费用的权衡。可靠性要求与性能、费用的权衡一般通过效能与费用分析、备选方案分析以及寿命周期费用分析等工具来实现。如采用备选方案分析,用半定量的或定性与定量相结合的方法对可靠性、性能和费用进行权衡分析。
- 可靠性要求与维修性、保障性要求之间的协调。在确定可靠性、维修性指标时,应根据战备完好性指标(如使用可用度 A_o),采用保障性分析来导出可靠性和维修性指标,或者通过建模与仿真方法对 RMS 指标进行权衡。
- 可靠性与安全性要求的协调。对于军用飞机、航天飞机或某些安全关键系统来说,规定了装备/系统的损失概率或安全可靠度指标,为了保证达到这些安全性指标,通常需要采用冗余、容错、隔离、监控、告警、逃逸等安全性设计技术。这将降低装备或系统的可靠性水平,因此,在规定安全性要求时,应进行权衡分析,以便协调安全性与可靠性要求。
- 基本可靠性与任务可靠性的协调。根据装备执行任务的要求以及保障费用的约束,在规定任务成功概率或平均致命故障间隔时间(MTBCF)的要求时,应通过权衡分析来协调 MTBF 与 MTBCF 的要求。为了提高系统的任务可靠性,必须采用冗余技术、增加系统的零部件数目,这些措施降低了系统的基本可靠性 MTBF,增加了备件数目和维修工作量,即提高了保障费用。通常应根据系统对完成任务的关键程度,在规定的保障费用约束下(即规定的 MTBF)来选择优化的 MTBCF,或者在规定的 MTBCF 下来选择优化的 MTBF。如远程运输机的任务持续时间为 10 小时,规定其任务可靠度为 0.9、MTBF=100h,按指数分布计算,可求得 MTBCF=95h,显然,其 MTBF 与 MTBCF 不协调。根据任务持续时间要求,MTBCF 可以小一些。
- 合同要求与使用要求间的协调。在合同中规定的 RMS 要求是根据定购方提出的使用要求文件中对 RMS 要求导出的,通常采用质量功能展开方法或要求转换方法来规定合同中的 RMS 要求。为了保证它们之间的协调,在进行要求转换时,必须全面考虑装备的使用方式、环境因素、维修及保障条件、工作持续时间、系统运行占空比 K 及维修与保障的管理等因素的影响。例



如,某装备的使用要求文件规定使用可用度 $A_o=0.8$, 经过转换后写入合同的可靠性及维修性要求分别为 $MTBF=5h$ 、 $MTTR=3h$ 。这说明合同要求与使用要求之间不协调,其原因是参数转换不当,或可靠性(及维修性)与可用性之间未进行权衡。

④ 产品可靠性论证,装备 RMS 要求确定的一般程序是从顶层到底层(自上而下),从总体/宏观到具体/详细,而且随着装备研制的进展,不断明确要求和细化要求。

⑤ 对软件产品或产品的软件部分的可靠性应进行专题论证,提出软件部分定性和定量的可靠性要求。

⑥ 可靠性要求论证报告须经专家评审,并作为产品立项报告和可行性研究报告的一部分。

⑦ 做好寿命周期可靠性规划。产品寿命周期内不同阶段的可靠性要求是不同的,因此,应合理规划产品寿命周期内每个阶段(包括处置阶段)的可靠性要求,这是研发一个成熟产品各个阶段所考虑的问题。需要对产品寿命周期内包括设计定型、批生产、运输、储存和使用运行等阶段的可靠性要求进行充分论证,给出科学的规划,以便使其在寿命周期各阶段承受的给定应力下能够达到期望的可靠性水平。寿命周期可靠性规划应覆盖产品寿命周期的各个阶段,包括前期的失效和后期的磨损。在产品寿命周期内,方案/规划阶段是建立表征不同应力特征的可靠性目标 and 要求的时段。产品在任何时间(如运输、储存、运行)都会承受应力,都有发生故障的可能。有时,产品在非工作时间遇到应力比工作时所遇应力危害还要大。在计划和确定产品合适的可靠性目标和要求时,要充分考虑这些因素。以美军装备型号为 AGM-86B 的巡航导弹为例,其可用度 A_o 规定形成首次待命能力的可靠度为 0.87 (1981 年 12 月);形成初始作战能力的可靠度为 0.90 (1984 年 12 月);可靠度目标值为 0.93 (1989 年 12 月)。

⑧ 确定可靠性要求时应同时明确如下条件:

- 寿命剖面。寿命剖面按时序完整描述了产品从投入使用到寿命终结或退役的整个过程所经历的各种有关事件及状态。例如,飞机在整个寿命期内所经历的每一重大事件,一般包括首飞、调整试飞、定型试飞、交付转场、试用、完成规定任务、维修保养、停放、大修、退役和其他可能的事件。寿命剖面描述每一事件的持续时间、环境条件和工作方式等。
- 任务剖面。任务剖面按时序全面描述了产品在完成规定任务这段时间内所经历的事件和环境。例如,飞机的任务剖面包括起飞、爬升、巡航、完成规定任务、返航、下降、着陆等各阶段所经历的高度、速度、持续时间、环境条件等。对于具有多任务能力的飞机,需要制订多个任务剖面,应规定多个可靠性指标。此外,任务剖面还需要说明产品的工作时间或占空系数。例如,F-

16 战斗机要求完成空对空和空对地作战任务,因此,需要制订空对空和空对地的任务剖面,其机载雷达的 MTBF 也规定了 2 个门限值,总工作状态的 MTBF_总=60h,空对空工作状态的 MTBF_{空对空}=70h。此外,任务剖面需要说明产品的实际工作时间与飞行时间的比值 K (占空系数),例如, F/A-18 飞机的电源系统的 K 值为 1.45,而起落架操纵系统的 K 值小于 0.2。任务剖面中,使用环境的描述很重要。环境特征描述用来确定客户将产品投入使用后产品所承受的工作和环境应力。如果对产品所承受的应力不清楚,那么所定的可靠性目标,不管是明确的还是隐含的,都没有意义。例如,某一产品在客户家里使用时,具有 500 小时 MTBF (平均故障间隔时间),但在环境应力较大的汽车里使用时,却只有 200 小时的 MTBF。在高层次产品中,环境可以表述为地面环境、移动环境、机载环境、空间环境等。但这只能大致提供产品所受应力范围的严酷情况。在设计过程开始的时候,需要知道更详细的信息。对于许多恶劣环境,使用仪器设备来测量期望的应力水平比较合适。例如,可用时间应力测量装置测量和记录如温度、湿度、冲击、振动和动力所导致的应力。

- 故障判别准则。这是可靠性鉴定和验收的依据。在对产品进行可靠性鉴定、验收或现场试验前,都必须根据产品类型及任务要求,制订故障判别准则,并对允许降级使用的要求给出规定,而且在故障判别准则中还应包括产品的性能参数和允许极限。
- 使用和保障方案。这是规定可靠性要求的重要考虑因素。使用方案包括用途、使用和部署、寿命剖面、任务剖面以及使用要求;保障方案描述为完成保障功能在各维修级别采用的机构、方法和技术,包括产品的维修等级、维修策略、维修任务、维修深度以及所需的保障资源,是在使用环境下对产品进行维修和保障的总体安排,说明产品在各个维修级别实施维修和保障的一般途径、每一维修级别的维修责任范围和所需的人力资源。使用和保障方案将影响产品及其保障系统的设计和布局,进而影响产品可靠性要求的确定。
- 指标实现时机。在确定可靠性指标时应明确哪一阶段或哪一时刻达到。例如,可靠性目标值一般应是产品已达到规定的设计能力,其可靠性增长已基本结束,且维修和保障设备已配套齐全时的可靠性水平,与产品的复杂程度、利用率及部署数量等各种因素有关。例如,美国空军 F-20 战斗机的可靠性目标值平均故障间隔飞行小时 (MFHBF) 为 4.2 小时,要求在累计飞行 10^5 飞行小时后达到;而 B-1B 轰炸机的平均维修间隔时间 (T_{BM}) 为 2.0 小时,要求在累计飞行 2×10^5 飞行小时后达到。因此,合同应明确规定指标实现的阶段和时机,即规定验证的时间。
- 验证方法。应根据产品的特点、产品层次、重要程度、经费和进度等因素明确指标的验证方法,即采用内厂试验还是现场使用 (或两者相结合) 验证。例如, F-20 战斗机的 MFHBF=4.2 小时,空军要求累计飞行 10^5 小时后达到。而



F/A-18 战斗机的门限值 MFHBF 为 3.7 小时,规定在累计飞行 2.9×10^3 小时后,用一架飞机进行 50 次飞行,每次飞行 2 小时,用点估计值表示法进行验证;F/A-18 的型号为 APG-63 的火控雷达的最低可接受值 MFHBF 为 64 小时,要求采用第 100~125 台中的产品,利用 MIL-STD-781B 中的统计试验方案进行可靠性鉴定试验进行验证。RMS 目标值一般应为装备达到成熟状态的外场统计值,美国空军规定装备形成初始作战能力后 2 年将达到成熟状态。由于不同类型装备的复杂性、利用率及部署的数量等因素存在差异,其达到目标值的时间也不同。此外,在规定装备的战备完好指标时,应明确装备的利用率,例如,规定陆军 RAH-66 直升机的战时使用可用度 $A_o=0.75$ 时,其利用率为每天飞行 6 小时。

4.6 确定可靠性要求及其验证的一般程序和方法

可靠性要求的确定过程,是一个综合论证过程,不能一蹴而就。可靠性要求的确定是装备 RMS 要求论证的重要组成部分,必须与相关要求的论证一起协调进行,必须经历一个由初定,经过反复协调、权衡,最终确定的过程。图 4-1 以军事装备为例,给出了可靠性要求的确定过程。

任务可靠性和基本可靠性分别源于任务成功性和战备完好性,对于一个装备,影响其任务成功和战备完好的因素很多,准确建立可靠性与它们之间的关系是一项很复杂的工作,工程中通常通过自上而下,自下而上反复模拟,即建模与仿真的方法来确定可靠性要求,一般过程如下:

① 根据基准比较系统可借鉴的数据和拟采用的技术改进,估计给出新研装备分系统(如机体、火控系统等)的可靠性和其他相关特性(如维修性)的初始值。

② 根据分系统的初始值,归纳求出整个装备的可靠性及其相关特性的水平(使用值与设计值)。

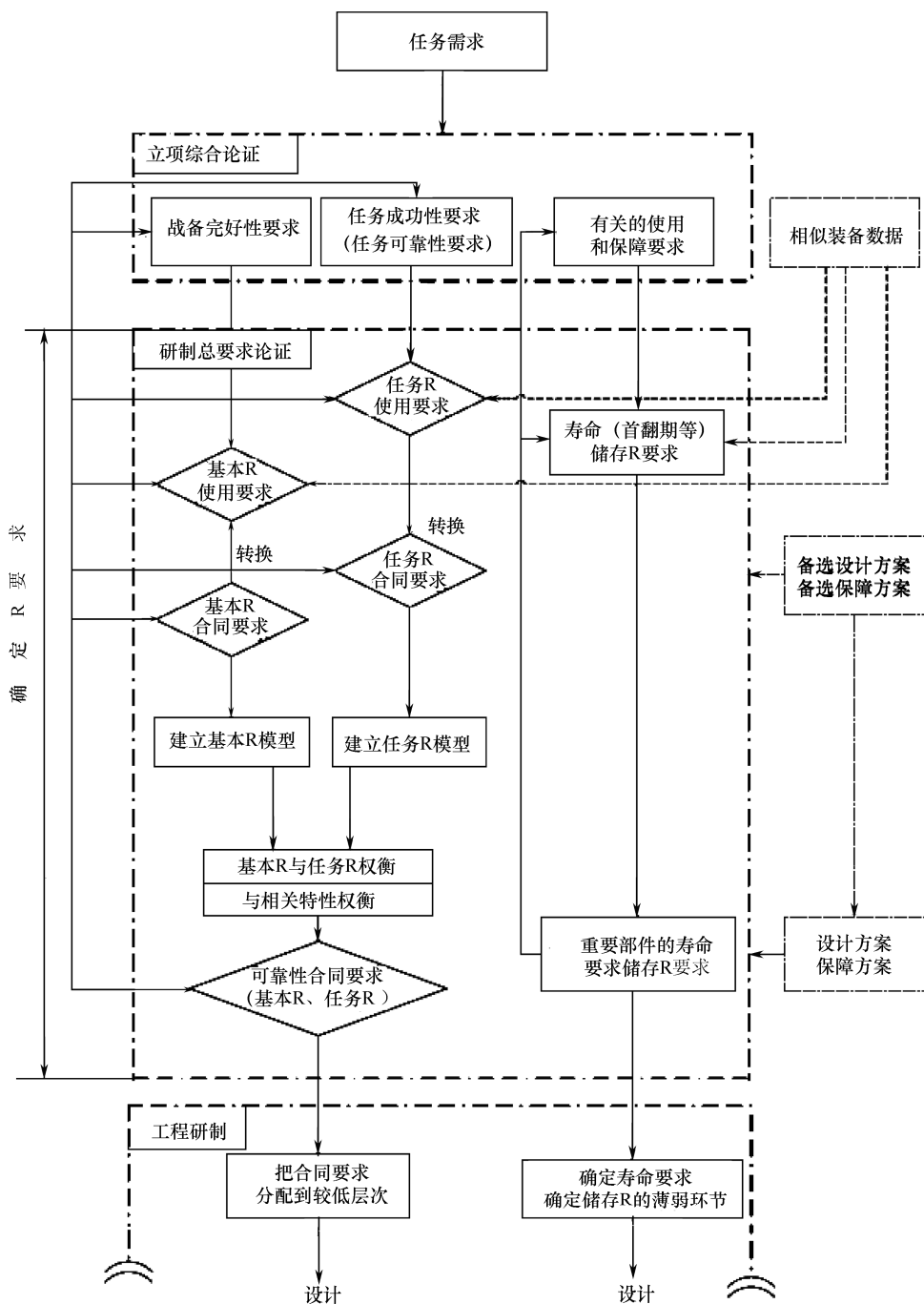
③ 根据相似装备的保障情况,估计可以实现的新装备的保障能力(如平均不能工作时间等)。

④ 建立可靠性(及其相关特性)、保障系统(包括保障资源)与战备完好性和任务成功性之间的仿真模型。

⑤ 进行仿真,确定能达到的战备完好和任务成功水平。

⑥ 调整可靠性和相关特性数据,以获得既能满足战备完好和任务成功性的目标,在技术上又能实现的可靠性要求。

表 4-5 给出了产品可靠性要求确定与验证的主要工作。



注：图中，“R”是“可靠性”一词的简写。

图 4-1 可靠性要求的确定过程

表 4-5 可靠性要求确定与验证过程的主要工作汇总表

阶 段	具体时机	工作项目	工作内容	输 出 到
论证阶段	装备立项综合论证	提出初步的 RMS 顶层使用要求	<p>① 根据作战任务需求，执行 GJB 1371 给出的 200 系列工作，如使用研究、比较分析、保障性和有关保障性设计因素等分析工作，提出新装备初始的可靠性、维修性、保障性（RMS）的顶层使用要求</p> <p>② RMS 顶层使用要求主要是指装备的战备完好性要求、任务成功性要求（或任务期间不能维修时，可直接提出任务可靠性要求），以及有关使用、保障及费用方面的要求或约束</p> <p>③ RMS 要求的论证是装备战术技术指标论证的一部分，必须将初定的战备完好性要求、任务成功性（任务可靠性要求）要求，以及有关的使用和保障要求纳入装备的立项综合论证报告</p>	立项综合论证报告
方案阶段	装备研制总要求论证时	提出并权衡可靠性使用要求和可靠性合同要求	<p>① 根据初定的装备顶层 RMS 使用要求，参考相似装备的数据，确定装备的初始可靠性使用要求。包括：由初始的战备完好性要求导出初始的基本可靠性使用要求，由初始的任务成功性要求导出初始的任务可靠性使用要求，由有关的使用和保障要求等提出初步的寿命和储存可靠性要求</p> <p>② 将可靠性使用要求转换为可靠性合同要求。利用经验系数或转换模型，将初定的可靠性使用要求转换为初定的可靠性合同要求，应注意确保转换的正确性和合理性</p> <p>③ 分析可靠性合同要求实现的可行性。利用备选的设计方案，通过建模、分配和预计等工作，结合相似装备的数据，分析新装备可靠性合同要求实现的技术、经济可行性</p> <p>④ 当可靠性合同要求难以实现时，通过调整可靠性与相关特性的要求，进一步完善设计方案等途径，重复上述步骤，使合同要求得以满足为止</p>	研制总要求
	装备研制总要求论证结束前	最终确定可靠性使用要求和可靠性合同要求	<p>① 最终确定的可靠性要求与相关特性的要求是相互协调的，并能满足战备完好性、任务成功性和有关的使用和保障要求</p> <p>② 最终确定的可靠性要求（使用的、合同的）应与相关要求一起纳入装备研制总要求论证报告</p>	研制总要求
工程研制与定型阶段	装备研制阶段初期	可靠性分配	将合同要求的可靠性指标分配到较低层次的产品	可靠性分配报告
	装备设计定型时	验证可靠性合同要求	在设计定型时，应按合同规定的验证方法，验证装备及其关键设备是否满足规定的可靠性合同要求。当不能满足时，应查明原因并提出解决途径	可靠性验收和鉴定试验报告

(续表)

阶 段	具体时机	工作项目	工作内容	输 出 到
生产与使用阶段	装备试用时	评价是否能满足可靠性使用要求	设计定型后，利用小批量生产装备进行试用时，应将是 否满足可靠性使用要求作为评价的内容之一。当不能满足 时，应分析是规定的可靠性使用要求难以实现，还是使用 要求转换为合同要求时有较大的误差，查明原因后，提出 解决办法	产品试用 报告
	在装备初始部署后	应验证可靠性使用要求	在装备的使用中还应进一步评价其使用可靠性。可靠 性使用要求的验证应与系统战备完好性评估一起，作为 初始能力评估的一部分，一般应在装备部署一个基本作 战单位、人员经过了规定的培训、保障资源要求配备到 位后进行。当可靠性使用要求不能满足时，应查明原 因，提出解决途径。装备投入使用一段时间后应进一步 评价装备的使用可靠性，为装备的使用可靠性改进和新 装备的研制提供信息	产品使用 可靠性评估 报告

上述程序和方法是以军用装备为对象给出的。为不失一般性，下面探讨商业产品的可靠性要求确定方法。

不像对大多军用产品或合同研制民品，一般都非常明确地指定定量的可靠性要求，许多商业产品的客户，不会明确指定他们对产品的具体要求，尤其是在可靠性方面。当客户不明确指定产品的可靠性要求时，供应商就需要运用各种方法和渠道来进行确定。

确定用户需求是导出使用可靠性要求和后续设计要求的基本前提。如果设计达不到这些需求，产品在市场领域就很难立足。包括可靠性要求在内的客户需求应尽可能早的确定，一般应在时间和资源大规模投入之前的产品研制过程的方案/规划阶段确定。客户需求是导出可靠性要求的先决条件。而可靠性要求，又是确定设计要求的重要基础之一，必须在产品设计开始之前确定。确定客户需求可能用到的方法主要有以下两种。

1. 市场调查

市场调查是了解客户对新产品（或改进产品）的要求和需求的有效途径之一。一般而言，客户会从产品的基本功能、质量、外观和使用年限等方面提出期望或具体特定要求。要深入了解客户需求，最好的方法就是广泛征询各层次客户意见，并对得到的反馈意见进行汇总和统计分析。当然，市场调查也会受到一些偏见和抽样误差的影响，周密的工作规划和采用适当的数据处理方法（如离群值的剔除）将有

效消除这些影响。

市场调查通常在产品的方案/规划阶段进行。当产品样品设计出来后，也可对不同的样品和设计方案多方征求领域专家和潜在客户的意见。在这种情况下，被调查的客户可能及时提供喜欢还是不喜欢的真实反馈意见。这有助于在产品全面研制、批量生产之前进行方案优选和设计改进。

2. 基准比较法

顾名思义，基准比较法是建立在与具体的基准比较基础上的，因此，选定基准是最为关键的一环。在产品开发过程中，一般将同类相似产品中被认为是一流的机构或最有力的竞争者作为基准。基准比较法就是将本公司的产品、服务、过程与选定的基准进行比较，从而确定待研发产品的目标和要求。其主要目的是对本公司的产品、服务、过程进行改进，以便赶上或超过作为基准的竞争者。通过比较，使供应商更加了解市场需求，以便在市场竞争中处于优势地位。注意，对基准的比较必须是全方位的，如果只注重某一方面，而忽略了其他某些重要的方面，很可能达不到预想的效果。例如，仅仅是某项性能，或者维修服务做到比同类的竞争者好，而忽略了其他方面——如外观和耐用性等，并不足以赢得竞争。

针对特定的产品，基准比较法可以帮助公司了解一流产品性能和可靠性水平。对产品性能与可靠性水平的了解和处理应放在产品的具体设计开发之前，应在产品开发的方案/规划阶段进行。通常，公司为了与竞争者的产品进行比较，会购买此产品的样品进行一系列的分析和试验，包括耐环境试验、可靠性试验等。进行试验的目的是为了确定产品的设计特性，包括材料选择、设计范围和公差、设计方法，以及可能的制造和装配方法。通过试验可帮助公司了解产品的工作特性、性能和可靠性水平。

产品策略也很重要。相对于一流产品，公司必须决定是否尝试进行竞争、赶超，还是设计成稍低于其性能的产品。如果给出第一种选择，一流产品的可靠性将作为最低要求。如果管理者认为产品可靠性水平与一流产品差不多，但是产品成本较低，以此来有效扩大市场份额的话，那将选择后一种方案。

基准比较法不但适用于确定产品级可靠性要求，而且也适应于确定较低级部件可靠性要求。另外，它还可以指导制订制造、装配，以及其他提高产品性能、降低总费用的商业管理行为的具体要求。

参 考 文 献

[1] GJB 450A-2004. 装备可靠性工作通用要求.

- [2] QRMS-55 GJB 450A. 装备可靠性工作通用要求实施指南, 总装备部电子信息基础部技术基础局和总装备部技术基础管理中心, 2008.
- [3] 韩坤, 刘维维. 装备 RMSST 定量要求论证方法. <http://home.cetin.net.cn/qrms/show.php?contentid=1402>.
- [4] 国外武器装备 RMS 要求论证中几个问题的探讨, <http://www.doc88.com/p-089786872647.html>.
- [5] 陈志田, 段鸿杰, 王利军. 可靠性要求论证方法. 质量与认证, 2015 年第 1 期, 50~52.
- [6] 任占勇. 军用飞机可靠性维修性指标确定方法. 航空标准化与质量, 1999 年第 1 期, 36~40.

第5章

可靠性设计分析

5.1 可靠性设计分析概述

5.1.1 目的

在论述可靠性设计分析的目的之前，让我们用一个简单的例子说明可靠性设计的内涵及其作用，以帮助大家了解可靠性设计分析的本质。

【例 5-1】防盗门对讲门铃开锁电路

图 5-1 (a) 是某住宅小区防盗门对讲门铃的外形图，图 5-1 (b) 为电磁锁开锁电路原理图。

上述设计从功能上看，完全没有问题：电路简单，实现开锁功能。但是，从可靠性视角，则存在明显的缺陷：当有人长时间按住按钮时，线圈或电源模块可能会发热，极易烧毁电路。这样的电路看似满足功能需求，但容易损坏，其结果必然是住户和管理者都不满意。对用户而言，三天两头门铃就坏了，不能正常使用；对管理者而言，经常被投诉，且维修成本高。

图 5-1 (c) 是经过可靠性分析后，改进的对讲门铃的电磁锁开锁电路设计。改进后的电路增加了一个限流电阻 (R_1) 和一个储能电容 (C_1)，可有效防止住户长时间按住按钮时电路模块的发热现象，保证门铃系统的经久耐用。

由此可见，可靠性设计并非可有可无，它是产品或系统设计必不可少的一部分，是保证设计生产出来的产品或系统既满足功能要求，又持续可用的重要手段。

这样的设计缺陷案例很多，小到上述的门铃电路，大到汽车、飞机、火箭和航天器。国内外大量的重大事故案例分析说明，由于产品设计时对可靠性考虑不充分，留下事故或安全隐患，最终酿成重大的事故，导致人员伤亡和财产损失。众所周知，美国挑战者号航天飞机爆炸事故，源于助推火箭的密封圈设计上的缺陷。一

般的民用工业和日用产品，如汽车前轴断裂、工程机械发动机飞轮开裂等事故，同样会导致人身伤亡和经济损失。如果在设计时留下不可靠的隐患，在产品生产出来后再予以弥补（如果可能），由此导致的故障损失和改进成本，往往需要花费成倍的代价。

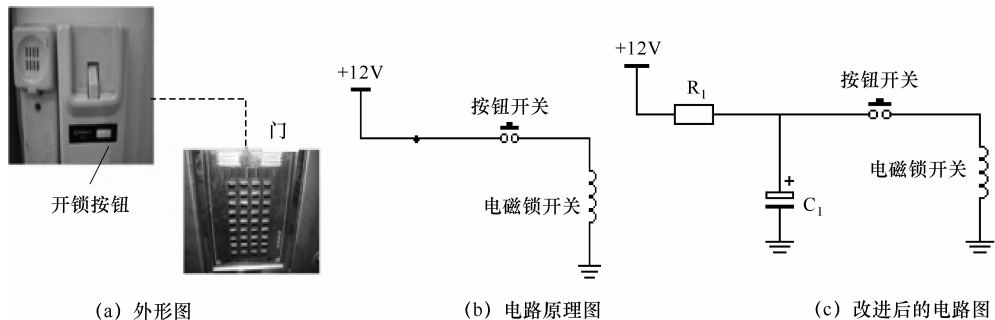


图 5-1 对讲门铃及其电磁锁开锁电路

统计数据表明，由于设计错误或缺陷导致的故障占比相当高。根据国内外航天器的安全事故统计数据，底层设备或元器件失效导致的仅占 14%；设计错误或缺陷导致的安全性事故占 39%，而很多操作失误（占 8%）与人机操作界面的设计不当有关，这两部分累加占 47%，接近 50%（参见图 5-2）。

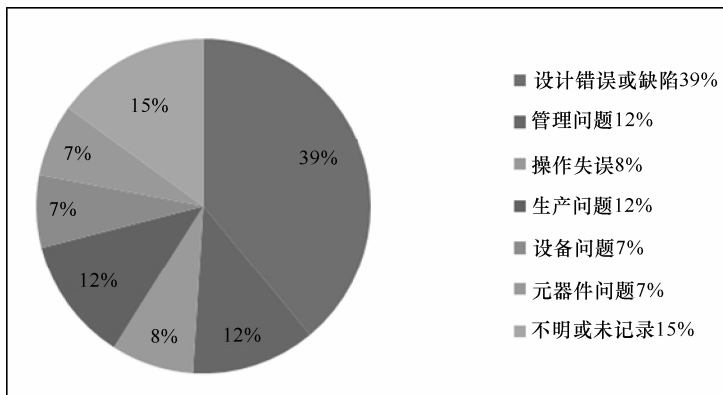


图 5-2 航天器安全事故原因分布

其他产品或系统的故障数据统计结果与上述结果相近。例如，根据对目前世界上商业运营的 5 座核电站系统安全事故记录的统计，部件失效导致的仅占 18%，系统设计缺陷、操作失误、书面规程的错误占比和不明原因的失效占比接近 60%。据日本对形成产品故障的原因调查分析，因设计不良引起的故障占 50%，元件、材料不良占 37%，而制造不良的原因占 13%。

从上述统计数据可见，50%的产品故障是由设计错误或缺陷导致的。由此不言

而喻，产品的可靠性设计是多么重要。

“产品的可靠性是设计出来的，生产出来的，管理出来的”，这是我国著名科学家钱学森同志在一次国防系统可靠性工作会议上作出的精辟论断。大家知道，产品的功能特性在设计阶段就被确定下来。同样，作为产品的固有特性之一，可靠性也在设计阶段就初步确定了，因此，可以说可靠性是设计出来的。一些人认为，产品的可靠性是通过一系列的试验、使用和数据收集，通过统计评估计算出来的，因此，觉得产品可靠性是试验评估出来的、使用统计分析得来的。这是认识上的偏差，因为试验和使用可靠性评估，只是对设计、生产出来的产品的可靠性进行验证和客观的评价，这些活动并不能形成或改变产品固有的可靠性。

顺便解析一下，可靠性是生产出来的，大意指的是在产品生产过程中通过对原材料、工艺的设计和控制，实现产品可靠性目标；而可靠性是管理出来的，说的是可靠性管理贯穿产品整个寿命周期，包括产品论证、设计、生产和使用维护整个过程，一系列与可靠性相关的组织和技术工作，需要有效的管理作为实施的保证。国内工程界有“三分技术，七分管理”一说，强调的就是可靠性管理的重要性。

自 20 世纪 40 年代末可靠性工程诞生至今的 70 多年中，产品可靠性设计就一直是其最为重要的组成部分。而可靠性分析是进行可靠性设计的前提，只有经过充分的分析，才能采取有效的可靠性设计措施。

产品的可靠性，设计是源头。在产品的设计过程中需要贯彻相应的可靠性设计理念，在产品功能等特性设计的同时进行可靠性设计。

可靠性设计与分析的主要目的是在产品研发的早期阶段，将问题或隐患消灭在图纸或技术文件上，以实现高可靠性、低寿命周期费用，以便满足用户需求。

5.1.2 一般程序和主要方法

可靠性设计的内涵是什么？产品的可靠性又是如何设计出来的？

简而言之，可靠性设计就是以赋予产品可靠性为目的而进行的设计。进一步可理解为，用合理的费用设计出符合可靠性要求的产品，并使其可靠性得以保持的一系列技术活动。可靠性设计分析的任务是分析、预测和预防产品所有可能发生的故障，使其达到规定的定性或定量的可靠性目标。

产品可靠性设计分析的一般程序如下。

1. 定义被设计分析的对象（产品或系统）

首先应明确被设计分析的对象，清晰地界定其边界。例如，对卫星系统而言，需要明确是单个卫星还是星群，是否包括地面接收系统和相关的数据链等。

2. 熟悉被设计分析的对象

这一步很重要，可靠性设计分析与确定的对象是密切关联的，是针对选定的对象进行的。因此，必须全面了解和消化被设计分析对象的技术规范、设计方案、图纸等技术资料。这样才能有针对性，做到有的放矢。

3. 收集和准备相关资料

收集与被设计分析对象相关的资料，包括其相似产品、其组成部分的相似产品、采购设备或系统的可靠性信息（如故障模式、失效率数据等），为可靠性设计分析准备基础数据。

收集数据时，前人的失败经验反馈非常重要，这是保证产品可靠性的最直接的经验方法。所谓可靠性设计，就是要求在设计时能预测和预防产品可能发生的故障。要做到这一点，可通过一定的理论分析和试验手段，或者凭借个人和前人过去设计成功和失败的经验进行。成功的经验多半总结在设计规范和手册中，对于失败的经验往往不能引起重视，对于可靠性设计来说，这是极为重要的资料。因此国外企业十分重视对产品的失效分析和事例收集工作，汇编成事例集和失效预防手册，以供设计人员参考，避免同类或相似失效再次发生。

4. 建立被设计分析对象的任务剖面 and 寿命剖面

根据被设计分析对象的使用要求和寿命要求，建立其典型的任务剖面 and 寿命剖面，确定假设和约束条件，如环境条件、使用与维修方式、故障定义、保障条件和资源等情况。

5. 确定其可靠性指标或要求

可靠性指标或要求和产品的其他指标（性能参数，功能参数等）一起是在产品规划阶段应当研究论证、决定的设计目标。可靠性指标应符合产品的特点，可以是单一的可靠性特征值，也可以是由多个可靠性特征值构成的可靠性指标体系；可以是定量的要求，也可以是定性的。同时，可靠性指标应结合上一步确定的产品任务剖面 and 寿命剖面来描述，即应对不同的任务剖面 or 寿命剖面分别确定相应的可靠性指标或要求。

6. 制定并在设计过程中落实可靠性设计准则

结合被分析设计对象的特点，制定可靠性设计准则。准则内容包括该对象的可靠性设计原则、实施要求和注意事项，包括采用成熟技术、原材料和货架产品的控制、产品加固、降额设计、冗余设计、耐环境设计等方面的准则。可靠性设计准则应在产品的方案阶段着手制定，在设计过程中不断补充完善，并采用准则符合性检查和评审等手段保证准则真正落实到产品的设计中。可靠性准则的落实过程，就是产品可靠性形成的过程。

7. 建立可靠性模型

建立可靠性模型是在产品的初步构成方案确定后进行。所谓可靠性模型是表示系统与各构成单元之间可靠性逻辑关系的图（如可靠性框图、故障树、马尔可夫状态转换图、Petri 网等）及数学关系式（需要定量分析时）。可靠性模型是进行可靠性分配、预计、分析和方案设计的基础。

8. 进行可靠性分析与（方案）设计

（1）可靠性分配

将系统的可靠性目标值合理分配给各构成单元。例如，对于机械产品就是将整机的可靠性指标分配到各总成，再将总成的指标分配到各部件、零件。对于电子产品则是将总的可靠性指标按系统—装置（子系统）—模块（部件）—元器件这样的层次进行分配。分配到每一部分的指标即这部分的可靠性设计目标值。可靠性分配依照可靠性模型进行。

（2）可靠性分析

对产品的设计方案进行故障模式、影响分析或故障树分析，以便找出设计上的疏忽和薄弱点，从传统技术和可靠性技术上提出改进措施。在整个设计过程中，每形成一个改进后的新方案都要视情况进行全面的或局部的可靠性分析。

（3）可靠性预计

对每个设计（初步、中间和最终方案）都按照其可靠性模型进行可靠性特征值的估计计算，并与给定的可靠性指标相比较。如果设计方案的可靠性水平未达到目标值，则要再进行改进，甚至重新进行可靠性分配。这时计算出来的可靠性指标只是一种理论预测，有待于在试验或使用中验证。

9. 设计评审

在设计方案确定之后组织专家对设计的各个方面进行评议、审查，目的是为了发现设计缺陷，提出改进措施，确保设计质量。设计评审根据产品的重要程度和复杂程度，可以进行多次（初步方案、中间方案和最终方案的设计评审），也可只进行一次（最终方案的设计评审）。

10. 可靠性研制试验

在设计方案经设计评审确定之后，方可试制样机并进行性能与可靠性试验，以便在实际条件下暴露问题，然后再改进设计。通过设计—试验—再设计的循环获得必要的可靠性增长，才能使设计最终达到要求。

5.1.3 可靠性设计准则

可靠性设计是在产品的研究和设计中采取相应的措施，使产品的可靠性提高并

达到可靠性指标的一项活动。

可靠性设计准则很多，并且，针对不同的产品，其设计准则可能差异很大。下面，我们介绍一些通用准则。

可靠性设计技术和方法主要包括：降额设计、容差与漂移设计、储备（冗余）设计、电路结构简化设计、潜在通路分析、热设计、静电防护等。

1. 简单化和标准化

尽量采用功能简单的零件，尽可能减少零件数量，尽量采用已经成熟或标准化的零件和技术，目的是减少零部件发生故障的概率，保证整机系统可靠性目标的实现。

下面以电路简化设计为例，说明简单化的原则。在可靠性工程领域中，电路结构指的是电路元器件的构成、电路的复杂程度、电路元器件的运用状态，以及元器件所处的各种力学、气候和生物环境条件。换句话说，电路结构可靠性关心的是如何减少电路复杂性，如何减少故障影响，并关心电路中使用了哪些类型、品种、规格和多少数量的电子元器件（集成电路、分立半导体器件、电容器、线圈、电阻器、开关、接插件、电动机以及电真空器件等），这些元器件承受了多大的电流、电压或功率，处于直流、交流还是脉冲工作状态，受到多大的热应力，电路工作于实验室、地面固定、车载、船载、机载还是航天设备中，元器件在电路中的运用状态是否正确等。

电路结构可靠性设计的目的是在满足电路性能要求的前提下，用降低以元器件损坏性失效为特征的电路失效方法来提高设备可靠性。电路结构可靠性设计的内容涉及元器件选型、元器件的应力减额、电路简化、故障软化、抗暂态效应和安全设计等。

简化系统不易，简化电路更难。简化电路的目的是要减少元器件的数量。要大量减少元器件，除了尽量革除电路中那些作用不大的元器件外，还应不拘泥于原来的电路形式，主要从实现电路集成化、简化数字逻辑电路、简化模拟电路方面进行简化设计。

2. 降额设计

所谓降额设计，就是使元件或零件的工作应力小于额定值，或者提高零件承载能力的安全裕度，以达到延缓其参数退化、降低零件或元件的故障率、提高使用可靠性的目的。

对于重要的安全保持性零件，采用极限设计方法，保证在最恶劣的极限状态下使用也不发生失效和破坏。

在电路设计中，为提高装备的使用可靠性，必须实施元器件的降额设计，GJB/Z 35《元器件降额准则》给出了相应的要求。GJB/Z 35 规定了电子、电气和机

电子元器件（以下简称元器件）在不同应用情况下应降额的参数及其量值，同时提供了若干与降额使用有关的应用指南。

通常元器件有一个最佳降额范围。在此范围内，元器件工作应力的降低对其失效率的下降有显著的改善，设备的设计易于实现，且不必在设备的重量、体积、成本方面付出大的代价。

降额设计应按设备可靠性要求、设计的成熟性、维修费用、难易程度、安全性要求，以及对设备重量和尺寸的限制等因素，综合权衡并确定其降额等级。在最佳降额范围内推荐采用三个降额等级，分别是Ⅰ级降额、Ⅱ级降额、Ⅲ级降额。

3. 冗余设计

为了提高系统可靠性，在组成系统时，增补一些工作单元或后备单元，即使其中之一发生故障，整个系统照样也能完成规定的任务，这类系统称为储备系统。储备设计是提高系统可靠性的主要方式之一。大多数系统可以简化成由若干个工作单元组成的串联系统，而串联系统中各工作单元的可靠度必须高于系统的可靠度；对于可靠度低于系统可靠度的串联单元，若通过其他改进设计的办法仍不能满足要求时，就只有采用储备设计才能奏效。储备设计可在元器件、部件或组件，甚至在子系统的任一级中采用。

储备方式分工作储备和待机储备，工作储备又包括并联储备和表决储备，并联储备的特点是储备系统的构成单元都处于工作状态，但只要有一个单元能正常工作就能保持系统正常，如汽车的两个前灯。表决储备的特点是储备系统的构成单元至少有 3 个，当占多数的单元保持其正常功能时，系统才能正常工作，如核反应堆安全保护停堆系统有 3 个核辐射探测器，其中至少有 2 个正常时，系统才正常，这种情况称为 3 取 2 储备。待机储备系统的特点是在工作单元之外设置具有相同功能的备用单元，当工作单元发生故障时备用单元才投入使用，如汽车的备用轮胎，重要系统的备用电源等。

4. 热设计

对电子设备进行合理的热设计，是为了以较少的冷却代价获得高可靠性的电子设备。热设计的基本原则如下：

- 保证冷却系统具有良好的冷却功能，即要保证设备内的元器件均能在规定的热环境中正常工作。为此应根据设备（元件）的热损耗值、用途、温升、尺寸、重量、经济性、可靠性、安全性等因素进行综合分析后，选择最简单、最有效的冷却方法，同时要注意元器件的配置应符合散热要求，热回路上的热阻要尽量小等，使元器件在允许温度下工作。
- 对密封设备，必须同时考虑内部和外部的两种热设计方案，使其内部向外部传热的热阻减至最小。

- 要保证冷却系统工作的可靠性。不管环境如何变化，冷却系统在规定的使用期限内，其故障率应比元件的故障率低，在紧急情况下，也应具有最起码的冷却措施，关键部件或设备在冷却系统的某些部分遭到破坏或不工作的情况下，仍有继续工作的能力。
- 冷却系统要便于使用、维修，便于测试修理和更换器件。
- 冷却系统应结构简单、可靠、工艺性好、具有较好的经济性，其成本只能占设备成本的一定比例。

温度对半导体器件的影响最为敏感，半导体器件的故障率随温度的增加呈指数上升，其电性能参数，如耐压值、漏电流、放大倍数、最大功率等均是温度的函数。晶体管的电流放大倍数随结温的升高而增大，它将引起工作点的漂移，增益不稳定，可能造成多级放大器自激或振荡器频率不稳定等。当晶体管的结温升高时，会使穿透电流和电流放大倍数迅速增加，由于集电极电流增大，使结温进一步升高，从而又使电流增大，形成恶性循环，直至晶体管损坏。为此必须控制晶体管结温不得超过允许值。

温度对电阻器和电容器的影响也很大。温度的升高导致电阻的使用功率下降，温度对电容器的影响主要是降低使用寿命。通常认为，电容器在超过规定允许工作温度下工作时，温度每升高 10°C ，使用寿命就要下降一半，此外，温度的变化也会引起电容量、功率因素等参数的变化。

5. 容差与漂移设计

一个产品，在其性能指标有规定合格范围的情况下，应考虑容差与漂移设计。产品性能指标的合格范围是由使用要求决定的。当产品的某项性能取值超出规定的合格范围时，就导致性能超差或退化性失效。因此，需要通过容差和漂移设计，来确定参数波动的容许范围。

6. 失效安全设计

失效安全设计是指当设备或系统的一部分发生故障时，依靠产品的自身结构而确保系统、设备的安全的设计。例如，压力表的防爆塞、汽车的放气制动系统都属于这一类设计。

对于机械结构，应设计成即使不得已发生了疲劳裂纹等部分损伤时，能使这种损伤限制在极小范围内，一直到被检查出来之前，结构不会发生致命破坏或影响功能的变化，这也是失效安全设计方法。

7. 耐环境设计

通过对产品所处工作环境类型、严酷程度以及对产品影响的预测和评估，进行产品强度和寿命的设计。通过耐久性试验、寿命试验、环境试验等各种可靠性试验



手段对产品的耐环境进行验证、修正。利用这些试验数据，分析产品的故障、劣化和磨损等现象，进一步参照各种规范、技术标准进行设计，这是可靠性设计中最基本的方法。

强化耐环境设计，会受到经济承受性的限制，必须在两者中进行权衡分析。一般而言，考虑对产品在极端环境下采取保护措施，比强化产品本身的耐环境性更为经济。例如，可以在运输、搬运和使用中遇到高温、高湿、振动、冲击等情况时，装备调节器、缓冲器等保护装置。

8. 人机工程设计

人员的误操作是复杂系统可靠性与安全性的一个重要威胁，除人员自身的原因外，操纵台、控制盘以及操作环境也与人员误操作有密切关系。人机工程设计的目的，一是为保证系统向人传达信息的可靠性（如指示、显示装置的设计）；二是保证人向系统传达指令或直接操作的可靠性（如控制终端、操纵器的设计）。这两方面都是属于系统自身的设计。操作环境的设计，目的是为了使人物的工作环境适合人的劳动生理特点以便减小误操作概率。

另外还有一种防误操作的设计思想，即抗误用设计，在设计上采取措施使产品在使用者误操作情况下也不发生故障，目的是适应一些低水平的使用对象，所谓的“傻瓜照相机”就是采用这种设计思想，故也称防愚设计，对于家电产品和武器系统十分必要。

人机工程设计，有时也被称为人因工程，或者人的操作可靠性设计。

9. 静电防护

尽管有些对静电敏感的微电子器件内部已采取了防静电设计，但其防护作用是十分有限的，所以在器件应用时，仍需采取各种有效措施，来防止器件受到静电损伤。总的防范原则，一是避免静电，即设法消除一切可能出现的静电源；二是消除静电，即设法加速静电荷的逸散泄漏，防止静电荷的积累。

由上可知，可靠性设计的涉及因素相当多，对于不同产品，不同的设计要求，采用的方法和贯彻的准则也不同。因此，有必要根据产品的特点制订专门的可靠性设计准则，并在设计过程中检查落实。

5.2 指导思想和原则

在上一节，我们探讨了可靠性设计分析的内涵、作用、一般程序、方法和准则。既然可靠性如此重要和必不可少，那么，要做好可靠性设计分析应考虑哪些因素、遵循什么样的思想和原则呢？

首先,可靠性设计分析是可靠性工程的重要环节,是一项集技术、管理和经验于一体,极富挑战性的工作。可靠性设计分析必须与产品研制密切结合,一般需要考虑下列因素:

- 产品的使用条件。
- 产品的性能要求。
- 产品的可靠性要求。
- 现有技术水平。
- 研制周期。
- 项目经费。
- 产品本身的特点,如体积、重量。
- 产品的使用维护、保障要求等。

产品的可靠性设计分析是在综合考虑上述因素基础上的系统性工作,既要满足性能指标和可靠性指标要求,又要考虑研制周期、经费和产品自身特点的约束,也就是说,它是对各项要素的一种综合与平衡。因此,在设计之初,必须全面对各要素充分分析和论证,确立正确的设计指导思想和原则,只有综合考虑、系统实施,才不会顾此失彼。可靠性设计指导思想和原则主要应包括以下几方面。

1. 充分分析、评估现有的技术水平

在限定的时间内,在现有的器材、线路和工艺水平下,研究出超现代水平的新技术是困难的。新技术的采用可能有利于满足性能指标和其他设计要求,但不可过于追求,必须充分估计在限定的研制周期内可能达到的实际水平。从可靠性、生产和使用的角度出发,应该尽量采用成熟的、定型的、标准的原材料、元器件、电路和工艺来完成设计。

【例 5-2】固态硬盘笔记本

在 2007~2008 年,有固态硬盘笔记本推出,有网络报道,某家大型计算机制造商发出的一份报告指出,该公司生产的固态硬盘笔记本,竟有高达 20%~30% 的回厂率,原因是主机频率和效能表现都不符合顾客期望。使用传统硬盘的笔记本,回厂率仅 1%~2%。除了价格和性能方面的原因外,有可能是该项新技术的不成熟和厂家对该技术认识验证不足,影响了其质量。

2. 准确掌握产品在运输、储存及使用中所遇到的环境和所处的状态

环境条件一般包括下述几个方面:

- ① 气候条件:温度、湿度、气压、盐雾及尘埃。
- ② 机械条件:振动(包括变频振动)、冲击、线加速度、噪声等。
- ③ 生物条件:霉菌、昆虫、鼠类等。



- ④ 电磁条件：电场、磁场及电磁辐射。
- ⑤ 核辐射条件：X 射线、 γ 射线、中子、质子、电子等辐射。

上述这些条件并不一定为每一产品所经历，重要的是设计者应明确产品实际所经历的是什么环境条件，以及产品的各组件对什么环境最敏感。设计者通过选取合理的设计方案和对各种耐环境设计技术——热设计、密封设计、减振设计、抗干扰设计和抗辐射设计技术的应用，就能使产品增强对环境的适应能力。

【例 5-3】变压器的外接线断

某设备的变压器，随机振动时，外接线从焊片处振断。主要原因是：次级输出直接从绕制引出端的焊片处引出，外接线未就近固定，加之剥线时对芯线的损伤，因此往往从焊点处折断。因此，所有孤立的单根或多根连接线，都应捆扎，就近固定牢靠，避免振动时导线发生相对位移。

3. 设计应满足工艺制造和调试检测的要求

在设计中，对影响产品可靠性的重要工艺，如电气连接（接触、焊点等）、表面处理（金属化孔、电镀等）、灌封和密封，以及工艺筛选和高温老化等应有规定。反之，制造工艺对设计也有一定的要求，例如：工艺过程中的高温环境，设计时是否已考虑？这些方面虽然设计者是熟悉的，但是否在设计的前期和方案阶段就进行这种考虑却是容易被忽视的。

另外，设计也应满足调试、检测及维护使用中的各种要求，如设计是否提供了方便的测试点，更换和调整的部位是否便于实施等。设计应综合考虑产品的工艺性、维修性和可靠性，要考虑调试、检测、维护和使用中涉及的人与产品的关系，有关这方面的内容称为人因工程设计；如何保证操作人员、设备和场地安全的有关内容就称为安全性设计。

【例 5-4】钽电解电容在随机振动试验中管脚折断

某设备的钽电解电容在随机振动试验中，其管脚被折断。通过调查分析，发现原因有 3 个：①电装时钽电容未紧贴印制板卧式安装；②电装后未用硅橡胶一类的材料将钽电容粘牢在印制板上或用卡子将钽电容卡牢在印制板上，使它们成为一个整体，以减少印制板的谐振数目，减轻共振的破坏；③安装尺寸设计不准确，电装前两端引线预处理不当。该钽电容是个头较大、重量较重的元器件，装上印制板后，若不采取加固措施，很难通过随机振动试验。只有上述 3 项安装工艺都到位，才有可能通过三个方向的振动试验。

4. 可靠性设计分析应与产品性能设计同步进行，反复迭代

必须牢固树立可靠性设计分析是产品设计不可或缺的一部分的思想，坚持可靠

性设计分析与产品性能设计同步进行的原则。任何试图把可靠性设计分析与产品性能设计割裂开来的思想都是错误的。一些人总是把可靠性设计分析放在产品性能设计之后,采用事后补救的方法试图提高产品的可靠性,结果往往事倍功半,顾此失彼,甚至造成无法弥补的经济或研制时间上的损失。

另外,可靠性设计分析除了应与产品性能设计同步外,还必须注意到,可靠性设计分析往往不是一蹴而就的,而是需要反复迭代,逐步提升,直到完全达到事先设定的要求。

5. 可靠性定量活动应贯穿产品研制和设计的始终

为保证产品设计时所考虑问题的全面性、各项设计要求的合理性和满足可靠性定量指标,必须在产品设计过程中进行一系列的可靠性定量活动、产品设计要求的分析和产品可靠性的具体定义、可靠性指标的确定和分配、方案和设计阶段的可靠性预计,以及可靠性论证等。

产品的可靠性定量活动应贯穿于研制阶段的始终,切不可一次“算总账”。虽然产品研制出来之后,进行一次评定能得到产品的可靠性数值,但这一设计可能不是一项合理的设计。

6. 定性与定量要求相结合

可靠性设计除注重有定量指标要求的设计外,还应注意定性的可靠性设计,做到两者并重、密切结合。

可靠性的定性设计一般通过制定一系列的可靠性设计准则,并在产品研制过程中执行来实现。由产品研制方或第三方对可靠性设计准则的符合性进行检查和审查,是落实可靠性设计准则的重要手段和保证。

7. 重视和加强设计阶段的可靠性管理

为确保设计质量和产品的可靠性,在研制设计中,必须贯彻和执行与可靠性设计有关的技术标准和规范、产品可靠性要求事项、可靠性工作计划,以及设计的可靠性审查程序等管理措施。可靠性设计并不是要求设计人员不遵循以往为保证产品性能指标有关的设计技术,而是要求在满足性能指标的同时,对各项技术的应用更加合理,并把提高产品质量和可靠性的一些经验,以标准和规定的形式固定下来,要求设计者必须遵守。

从上述一些观点出发,要求产品的设计人员掌握一定的可靠性设计的基本概念和可靠性设计技术,并把它运用到产品设计中去,完成各设计阶段中规定的可靠性要求,并通过规定的审查。为此,可靠性设计技术中的几个重点是:产品的可靠性定义和分析;系统可靠性的计算方法;可靠性分配方法;方案阶段的可靠

性预计法和设计阶段的可靠性预计法；与可靠性有关的设计技术；设计阶段的可靠性管理等。

5.3 可靠性建模

5.3.1 可靠性模型的内涵和作用

建立可靠性模型的目的是为了分配、预计和评估产品的可靠性。可靠性模型是开展可靠性分配、预计、分析和评估等工作的前提和基础。可靠性模型一般由两部分构成：

- 产品或系统与各构成单元之间可靠性逻辑关系的图（如可靠性框图、故障树、马尔可夫状态转换图、Petri 网等）。
- 相关的数学模型或计算机算法（如逼近算法或仿真计算程序）。这部分在定量分析计算时是必不可少的。

根据建立的可靠性模型、工作循环和任务时间等信息，拟定数学表达式或计算机程序，利用这些表达式和程序，以及相应的故障率和成功概率的数据，可进行基本可靠性和任务可靠性的分配、预计、分析和评估。

可靠性模型的建立，不是一定要等到产品的设计图纸完成后才开始，在产品的设计初期就应建立产品可靠性模型，以有助于设计评审，并为产品的可靠性分配、预计和拟定纠正措施的优先顺序提供依据。随着产品设计的深入、细化，可靠性模型也逐步细化。当产品设计、环境要求、应力数据、故障率数据或寿命剖面发生重大变化时，应及时修改可靠性模型。

可靠性模型分为基本可靠性模型和任务可靠性模型。下面分别对这两种可靠性模型进行阐述。

5.3.2 基本可靠性模型

基本可靠性的定义是：产品在规定条件下无故障的持续时间或概率。由基本可靠性定义可知：

- 基本可靠性与规定的条件有关，即与产品所处的环境条件、应力条件、寿命期有关，也就是与“寿命剖面”确定的条件有关。所谓的与“寿命剖面”有关，包括系统从出厂（交付用户）到退役这段时间内所经历的全部事件和环

境的时序描述。基本可靠性涉及寿命周期内所有寿命单位和所有引起维修要求的故障，即使任务未受影响，但对维修保障提出了要求的所有故障均应该考虑进去，它是影响维修保障费用的一个重要因素。

- 基本可靠性是“无故障的持续时间或概率”，它说明产品经过多长时间后可能要发生故障。这里，“时间”是一个广义的概念，它可以是小时，也可以是里程或其他寿命单位。“故障”是指引起维修工作的事件或状态。这种故障可能影响，也可能不影响产品完成任务的功能。

可见，决定基本可靠性的是产品在整个寿命期内发生的所有需要维修或更换的故障，而不局限于发生在任务期间的故障，也不局限于危及任务成功的故障。这些故障决定了维修频数、备件数量，因而，基本可靠性涉及维修人力费用和后勤保障要求。

基本可靠性反映了构成系统的所有单元发生故障都需要维修或更换，构成产品的所有单元都应包括在模型内，包括产品所有用于储备工作模式的单元，所以，基本可靠性模型是串联模型。基本可靠性预计是用串联模型来估计产品的可靠性。即使产品包含冗余或代替工作模式的单元，都要按串联处理。这是因为，冗余或代替工作模式单元所发生的故障虽然不直接影响产品功能，但它同样要排除，因此，组成系统的单元愈多，产品的基本可靠性愈低。

基本可靠性预计应全面考虑从产品接收至它退出使用期的可靠性，即应是寿命期的可靠性预计。产品在整个寿命期内除工作之外一般还有储存、运输、休眠等非工作状态，因此，产品的寿命期可靠度（基本可靠度）一般为产品工作状态下的可靠度与各种非工作状态下的可靠度之积。只有当产品的非工作状态故障率与非工作状态时间之积足够小、可以忽略时，寿命期可靠度才近似于工作期可靠度。

通过预计，若基本可靠性不能满足要求，可以通过简化设计，或采用高质量等级的元器件，或调整性能容差等措施来弥补，靠增加储备单元的方式不能提高基本可靠性，反而使其降低。图 5-3 为某型民用机场终端引导雷达系统的基本可靠性框图，从图中可见，组成雷达系统的各个设备可靠性逻辑关系为串联模型。

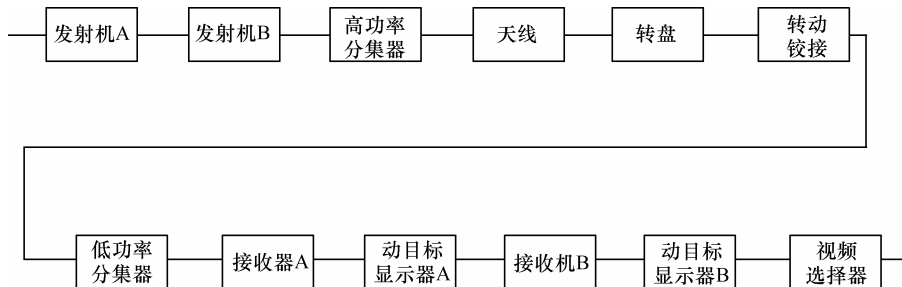


图 5-3 某型民用机场终端引导雷达系统的基本可靠性框图

5.3.3 任务可靠性模型

任务可靠性的定义为：“产品在规定的任务剖面内完成规定功能的能力”。

由任务可靠性定义可知：任务可靠性与规定的任务剖面有关，即与任务成功或失败的判别准则、任务时间及产品在任务期按时序所经历的应力条件、环境条件有关。

可见，任务可靠性反映了产品的任务成功性，决定任务可靠性的是产品在执行任务期间所发生的危及任务成功的故障。因此，确定任务可靠性时，只统计发生在任务期间的危及任务成功的故障。

任务可靠性模型应该描述在完成任务过程中产品各单元的预定用途、作用，包括用于冗余或代替工作模式，相应地，这些单元在模型中反映为并联结构或特定任务阶段及任务范围的类似结构，所以，建立任务可靠性模型的结构相对比较复杂。

在任务可靠性和基本可靠性模型中产品单元的名称和标志应当一致。在产品既没有冗余又没有代替工作模式的情况下，基本可靠性模型和任务可靠性模型的结构相同，都是串联结构。但前者的时间范围是整个寿命周期；后者的时间范围仅与任务时间相对应。

任务可靠性预计一般是采用复杂的串—并联模型来估计产品完成规定任务的概率。预计所采用的可靠性模型取决于产品功能原理、可靠性结构及产品各单元在执行任务过程中的不同作用。

产品增加冗余或代替工作模式单元，会提高其完成规定任务的可靠性，因为冗余或代替工作模式单元发生故障仅相当于暂缺该单元，但不影响其任务的完成。

任务可靠性预计应该涉及产品规范中规定的每一种工作模式，预计结果应该表明产品是否满足在每一种工作模式下的可靠性要求。

通过预计，若任务可靠性不足，可以通过适当的增加备份单元的冗余设计，或改善应力条件、优选元器件，或调整性能容差措施来弥补。例如，某民用机场终端引导雷达系统的任务可靠性模型如图 5-4 所示，该模型中，发射机、接收机、动目标显示器均备有冗余单元。

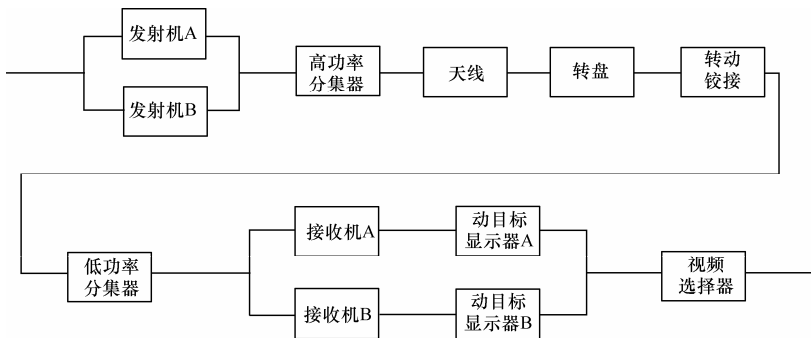


图 5-4 某型民用机场终端引导雷达系统的任务可靠性框图

5.3.4 基本可靠性与任务可靠性的区别和联系

在建立可靠性模型的过程中，很容易混淆基本可靠性和任务可靠性模型。从基本可靠性与任务可靠性的定义来看，两者的区别和联系在于以下方面。

1. 两者的时间界定不一样

基本可靠性与任务可靠性都强调无故障完成任务，但任务可靠性强调完成规定的功能是界定在“任务剖面”的范围内。基本可靠性强调的持续时间是界定在“寿命剖面”的范围内，一个“寿命剖面”一般包含一个以上的“任务剖面”，也就是说，一般情况下，基本可靠性界定的时间范围比任务可靠性所界定的时间长。

2. 两者的故障计算方式不一样

度量任务可靠性时只考虑影响完成任务的故障，而与任务无关的故障不考虑。基本可靠性涉及整个系统寿命周期内需要维修的故障，也就是说，不管故障对任务是否有影响都要考虑。

3. 两者的作用不一样

任务可靠性直接影响装备系统的作战效能。基本可靠性与维修保障有关，直接影响维修保障费用。

4. 两者的计算模型不一样

任务可靠性模型是用来估计系统在执行任务过程中，完成其规定功能的能力。因为任务可靠性强调规定的“任务剖面”和完成任务的能力，因此，建立模型最主要的问题是确定任务剖面。一个系统的基本可靠性框图是唯一的，而任务可靠性框图则因任务的不同而不同，应当根据不同的任务和任务剖面，画出其任务可靠性框图。如教练机在完成攻击任务时，其任务可靠性框图中必定包括火控和军械系统，而在完成其他非攻击任务时则不应包括它们；对其燃油系统来说，在完成航行任务时需带副油箱，此时任务可靠性框图中必须包括副油箱及其附件，而在进行起落训练时，不必带副油箱，因此可靠性框图中也不必包括副油箱。

5.3.5 基本可靠性和任务可靠性的权衡

要提高任务可靠性，可采用简化产品设计和采用高可靠性的元器件，既可提高

基本可靠性，又可提高任务可靠性，这是比较理想的情况。但是，实际上在产品的设计过程中，往往受限于元器件的工艺水平或其他设计要求，无法大幅度提高元器件的可靠性水平。此时，为了使产品的任务可靠性达到设计要求，需要采用一定的冗余设计手段，增加冗余单元以达到任务可靠性要求。但是，增加冗余单元后，必将降低基本可靠性。因此，产品设计时，需要在基本可靠性和任务可靠性之间找到一个平衡点。在权衡基本可靠性和任务可靠性指标时：

- 当任务可靠性相同时，基本可靠性高比较好。
- 若一个设计的基本可靠性比另一个高很多，即使任务可靠性稍低也是可取的。
- 若一个设计的任务可靠性预计不能满足合同要求，往往降低基本可靠性，以提高任务可靠性。

基本可靠性和任务可靠性的建模及预计都应尽早进行，并随着设计和信息的变化及时进行相应修改，为计划、决策提供有价值的信息。由于缺乏详细的设计资料，早期预计难免粗糙，但是，在可靠性指标分配方面，或在确定满足可靠性指标要求的可行性方面，可对设计师和管理人员提供有用的反馈信息。同时，应确切地分析、及时地反馈没有达到可靠性指标要求的信息，以便尽早制定其改进措施。改进措施制定得越早，就越容易实施，提高产品可靠性的效果也就越大。基本可靠性、任务可靠性的预计结果，还要与可靠性指标论证、分配、产品方案论证及可靠性设计评审等活动相结合，而且，往往需要交错、反复地进行。

5.3.6 建立可靠性模型的一般程序

1. 确定产品的定义

首先，必须清晰定义要建立可靠性模型的产品或系统，明确界定其边界。在此基础上，再熟悉产品和工作原理、性能、用途、使用维护条件和限制等，这是建立可靠性模型的前提。

(1) 确定产品的用途或任务，并了解其工作原理和工作模式

依据产品可靠性的定义可知，可靠性与产品的功能密切相关。而产品功能是产品的用途和任务关联。因此，确定产品的用途或任务，并了解其工作原理和工作方式，是确定产品的任务剖面或寿命剖面，进而建立相应可靠性模型的基础。

一种产品或可以用于完成一种以上的任务。例如，飞机可用于空中格斗、对地攻击、军事侦察或反潜等任务。如果用不同的飞机分别完成这些任务，就可用每一任务的或飞机单独的可靠性模型来描述这些任务。

有些多用途产品需要用不同的单元来完成多种功能，因此，这些产品具有多种工作模式。例如，在雷达系统中，搜索和跟踪就是两种工作模式。两种工作模式下的任务剖面不同，其可靠性模型也不尽相同。

在建立可靠性模型之前，必须说明需要完成的具体任务，如果任务分多个阶段且各阶段的工作模式不一样，则需要分阶段建立一组可靠性框图。

(2) 确定产品的性能、结构参数、允许极限，以及接口要求

建立故障判据是可靠性分析的前提之一。为了建立产品的故障判据，应规定产品的性能、结构参数及容许极限。产品的性能参数极限可以是功率、电压、容量、范围、速度等的阈值；而产品的结构极限包括最大尺寸、最大重量、人为因素极限、安全规定及材料能力等。最简单明了的方法是编制一个参数清单或图表，并应规定这些参数允许的上限和（或）下限。

当某产品依赖于另一个产品时，各产品之间的兼容性必须协调一致，即规定各产品功能之间的接口，如人机接口以及与控制单元、电源等之间的接口。明确接口的功能、要求是定义接口故障判据的前提。

2. 确定产品的寿命剖面

一般情况下，寿命剖面指的是对从产品出厂（被用户接收）到寿命终结或退出使用的整个过程所经历的各种有关事件及状态的全面时序描述。它说明产品在其整个寿命期内所经历的每一重大事件，如装卸、运输、储存、试验和检查、备用及待命状态、使用部署、任务剖面，以及其他可能的事件。寿命剖面描述每一事件的持续时间、环境条件和工作方式等。

例如，某雷达的寿命剖面如图 5-5 所示。该雷达的整个寿命剖面从产品交付开始，涉及装运、储存、启封、展开、任务剖面、站上维修、送厂翻修、任务剖面、站上维修、报废或退役为止。

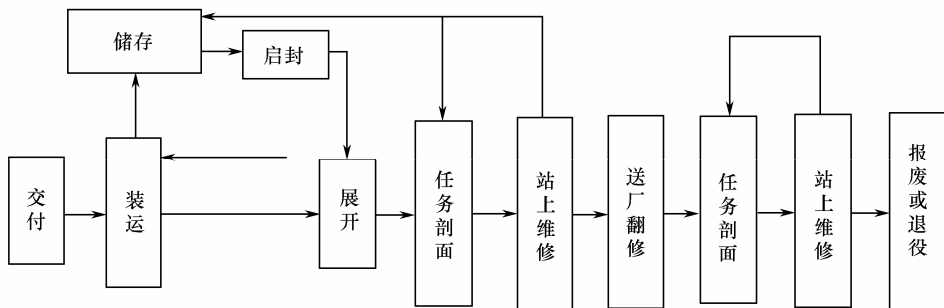


图 5-5 雷达寿命剖面

又如，图 5-6 是军用飞机的寿命剖面，描述了军用飞机从交付到退役、报废所经历的事件序列和环境，为军用飞机从交付到退役、报废所经历的典型事件，以时间为横坐标将图中的事件展开即为军用飞机的典型寿命剖面。

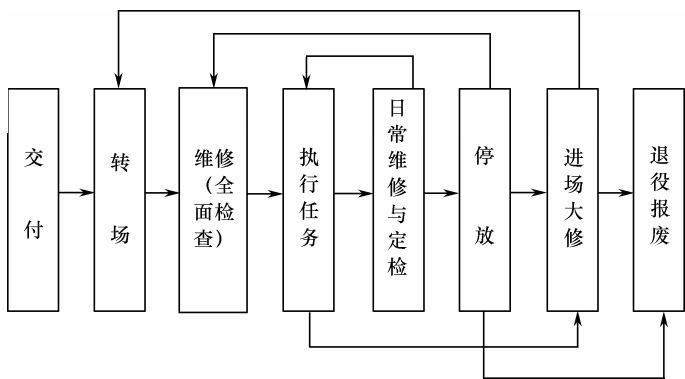


图 5-6 军用飞机的寿命剖面

产品的任务剖面是指产品在完成规定任务这段时间内所经历的事件和环境的时序描述。任务剖面是寿命剖面的一个组成部分。

以军用飞机为例，其任务剖面是在军用飞机执行典型任务过程中所经历的所有事件和环境，一般包括起飞爬升、出航、作战、返航和下降着陆等阶段。一种军用飞机的任务剖面由于执行的任务不同（如转场、巡逻、空战、对地支援、轰炸、侦察、运输、空降、空投等）可以有若干个，在论证时应选出考核时所使用的典型任务剖面，可以是一个或多个。任务剖面中应说明飞机的飞行状态、外挂构型等，外挂构型也可以是一个或多个典型构型。任务剖面还应该包括飞机的环境剖面，是在不同任务条件下的各种环境条件的变化时间历程，如飞行的高度（含气温、气压）、速度（含驻点温度、速压）、过载、震动（含抖动、炮震、落震）、电磁环境等。机载设备的环境剖面会因在机体中的不同位置及不同飞行状态而不同。

图 5-7 是某型歼击机的典型任务剖面示意图。

在实际应用过程中，往往许多人会把寿命剖面与任务剖面混淆。例如图 5-7 中的某型歼击机的任务剖面，一般是描述其在规定空空作战任务这段时间内所经历的事件和环境的时序。它与寿命剖面最大的区别是时间范围，任务剖面的时间限于规定的任务时间内，一般小于系统的寿命时间，而寿命剖面的时间范围是从产品交付直到系统报废或者退役。一般情况下，寿命剖面可包括多个任务剖面。

为确切描述产品的多任务能力，需要制定多种任务剖面。任务剖面需要说明产品的工作时间或占空系数。产品应细分为组成单元（或部件），并绘制曲线图，以表示每一单元在产品整个使用期间的用途。例如，飞机的起落架只有在飞机起飞及着陆时才工作，而在整个飞行期间是不工作的。因此，在建立可靠性模型时，必须加以修正，通常

用占空系数进行修正。占空系数为单元的工作时间与产品或系统的总工作时间之比。

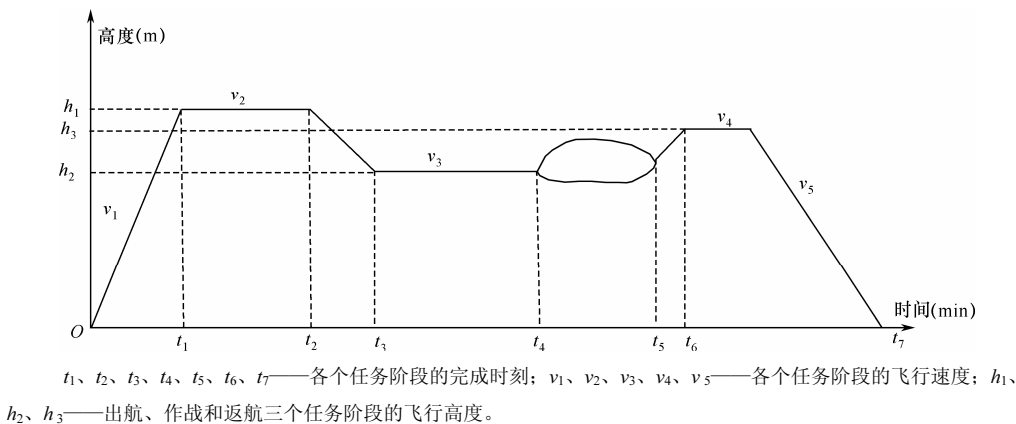


图 5-7 某型歼击机空空作战的任务剖面示意图

通常采用如下两种方法进行修正。

(1) 方法 1

在单元不工作期间的故障率可以忽略不计的情况下, 假设单元的故障时间服从指数分布。

$$R(t) = e^{-\lambda t d} \quad (5-1)$$

式中: $R(t)$ ——单元(或子系统)的可靠度;

λ ——单元(或子系统)的故障率;

t ——产品(或系统)的工作时间;

d ——占空系数, $d = \frac{\text{子系统工作时间}}{\text{系统工作时间}}$ 。

(2) 方法 2

在单元不工作期间的故障率与工作期间的故障率不同的情况下, 假设单元的故障时间服从指数分布。

$$\begin{aligned} R(t) &= R_1(t) \times R_2(t) \\ &= e^{-\lambda_1 t d} \times e^{-\lambda_2 t (1-d)} \\ &= e^{-(\lambda_1 t d + \lambda_2 t (1-d))} \end{aligned} \quad (5-2)$$

式中: $R_1(t)$ ——单元(或子系统)工作时的可靠度;

$R_2(t)$ ——单元(或子系统)不工作时的可靠度;

λ_1 ——单元(或子系统)工作时的故障率;

λ_2 ——单元(或子系统)不工作时的故障率。

因此, 需要同时进行工作状态和非工作状态的可靠性预计。

3. 确定故障判据

产品故障（或失效）指的是产品不能在规定条件下完成规定任务（或功能）的状态。依据上述章节建立寿命剖面（含任务剖面和环境剖面），利用确定的产品功能、性能和结构参数、允许极限，以及接口要求，列出所有可能造成产品故障的条件，即拟定产品故障判据。例如，雷达完成任务的一个条件是其发射机功率必须大于或等于 200kW，因此，导致发射机功率输出小于 200kW 的单一（或组合的）硬件或软件故障必定使雷达不能完成任务。

在某些情况下，虽然存在故障状态，但产品仍能完成任务。这样的故障在计算任务可靠性时就不应作为相关故障计算。

4. 绘制可靠性逻辑关系图

这一步需要在上述分析的基础上，根据产品的任务要求、工作方式和寿命（任务）剖面等绘制出表示系统与各构成单元之间可靠性逻辑关系的图。

可靠性逻辑关系图有多种形式，可以是可靠性框图、可靠性树（一种表示可靠性关系的树状图）、故障树或 Petri 网等。其中，最常用的是可靠性框图。

可靠性框图表示产品在寿命剖面中所有功能的相互关系及独立性。产品的所有储备及其他防止故障影响的措施也应在框图中表示出来，以便采用防止单点故障对更高一级的产品造成灾难性影响的措施。对每一工作阶段或每一工作模式需要绘制一个独立的可靠性框图，因为产品的用途及致命性可能随着任务阶段或工作模式的不同而变化。

【例 5-5】低频治疗仪可靠性框图的构建

图 5-8（a）是低频治疗仪的功能原理图。图 5-8（b）是根据其功能构建的可靠性框图。

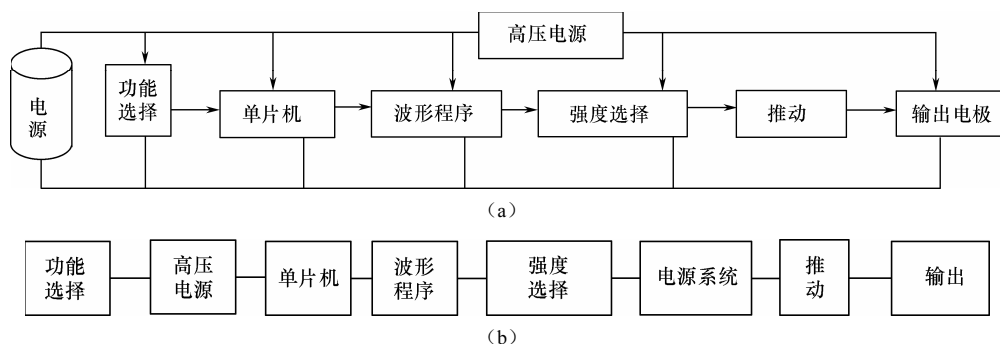


图 5-8 低频治疗仪的可靠性框图

可靠性框图只表明组成产品的分系统或组件与产品可靠性关系的连接，虽然它要根据产品的组成原理图来勾画，但它并不等同于产品组成原理图。要特别注意的

是,可靠性逻辑关系图一般不同于系统的工作原理图。前者反映的是系统可靠性的逻辑关系,后者描述系统的工作原理。通常,可靠性是产品组成子系统或组件的串、并联的某种组合。组件在串联环节中的相对位置是没有物理意义的,它只表明产品完成规定任务所必须保证的各功能组件的关系。

5. 建立可靠性数学模型

建立可靠性数学模型是进行可靠性量化分析(如分配、预计和评估等)的基础。根据产品的复杂程度,可采用不同的方法建立可靠性数学模型,常用的方法有如下几种。

(1) 普通概率法

利用普通的概率关系式,根据产品的可靠性框图建立可靠性数学模型。这种方法可用于单功能和多功能的系统。

(2) 布尔真值表法

利用布尔代数法,根据产品可靠性框图建立可靠性数学模型。这种方法比普通概率法麻烦,但在熟悉布尔代数的情况下,这种方法还是有用的。它适用于单功能及多功能的系统。

(3) 逻辑图法

逻辑图根据可靠性框图建立可靠性数学模型。这种方法比普通概率法麻烦,但它是布尔真值表法的简化方法,通过各项合并来简化任务可靠度公式。

(4) 蒙特卡罗模拟法

利用随机抽样方法根据可靠性框图进行可靠性预计。当已知产品中各单元的概率(或等效可靠性参数),但任务可靠性模型过分复杂,难以推导出一个可以求解的公式时,可采用蒙特卡罗模拟法。这种方法不是产生一个完成任务的通用公式,而是根据产品各单元的概率和可靠性框图,计算产品完成任务的概率。它适用于单功能及多功能系统。

5.3.7 典型的系统可靠性模型

1. 串联系统

定义:系统中的下属几个组件全部工作正常时,系统才正常;当系统中有一个或一个以上的组件失效时,系统就失效,这样的系统称为串联系统。串联系统的可靠性框图如图 5-9 所示。设系统下属组件的可靠度分别为 r_1, r_2, \dots, r_n , 串联系统的可靠度为 R_s 。

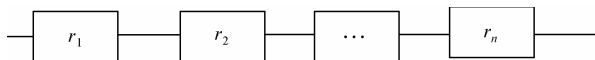


图 5-9 串联系统可靠性框图



可以证明, 串联系统的可靠度 R_s 为各单元可靠度的连乘, 即:

$$R_s = r_1 \cdot r_2 \cdots r_n = \prod_{i=1}^n r_i \quad (5-3)$$

一般情况下, 可靠度是任务时间的函数, 即 R_s 应表示为 $R_s(t)$, r_i 应表示为 $r_i(t)$, 对于指数分布有:

$$r_i(t) = e^{-\lambda_i t} (i=1, 2, \dots, n)$$

$$R_s = r_1 \cdot r_2 \cdots r_n = \prod_{i=1}^n r_i = e^{-\left(\sum_{i=1}^n \lambda_i\right)t}$$

即

$$\lambda_s = \sum_{i=1}^n \lambda_i \quad (5-4)$$

$$MTBF = \frac{1}{\sum_{i=1}^n \lambda_i} \quad (5-5)$$

式中, t 为系统的任务时间; $R_s(t)$ 为系统的可靠度; λ_s 为系统的等效故障率; MTBF 为系统的平均故障间隔时间; $r_i(t)$ 为第 i 个单元的可靠度; λ_i 为第 i 个单元的失效率, 下同。

2. 并联系统

定义: 系统中的几个下属组件, 只要其中一个工作正常, 则系统就正常工作, 只有全部组件都失效时, 系统才失效, 这样的系统称为并联系统。

并联系统的可靠性方框图为 n 个组件的并联图 (参见图 5-10)。设各组件的可靠度分别为 r_1, r_2, \dots, r_n , 相应组件的失效 (故障) 概率 (不可靠度) 分别为 f_1, f_2, \dots, f_n , 假设并联系统的失效 (故障) 概率为 F_s 。

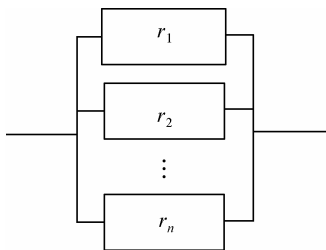


图 5-10 并联系统的可靠性框图

可以证明:

$$F_s = f_1 \cdot f_2 \cdots f_n = \prod_{i=1}^n (1 - r_i)$$

并联系统的可靠度:

$$R_s = 1 - F_s = 1 - \prod_{i=1}^n f_i = 1 - \prod_{i=1}^n (1 - r_i)$$

对于指数分布, 则有:

$$\begin{aligned} \text{MTBF} &= \int_0^{\infty} R_s(t) dt \\ \text{MTBF} &= \sum_{i=1}^n \frac{1}{\lambda_j} - \sum_{1 \leq i < j \leq n} \frac{1}{\lambda_i + \lambda_j} + \cdots + (-1)^{n-1} \frac{1}{\lambda_1 + \lambda_2 + \cdots + \lambda_n} \end{aligned} \quad (5-6)$$

当 n 个单元相同时:

$$\begin{aligned} \text{MTBF} &= \int_0^{\infty} \{1 - (1 - e^{-\lambda t})^n\} dt \\ &= \frac{1}{\lambda} + \frac{1}{2\lambda} + \cdots + \frac{1}{n\lambda} \end{aligned} \quad (5-7)$$

两个组件并联的可靠度为:

$$R_s = r_1 + r_2 - r_1 r_2 \quad (5-8)$$

而两相同组件并联的可靠度为:

$$R_s = 2r - r^2 \quad (5-9)$$

【例 5-6】带有并联结构的系统可靠性计算

计算机由电源、主板和显示器 3 部分构成, 为了提高电源的可靠性, 设计时采用 2 个相同电源并联。其可靠性框图如图 5-11 所示, 各组成部分的可靠度 (时间为 3 年) 分别为: $R_{\text{电源}}=0.6$, $R_{\text{主板}}=0.9$, $R_{\text{显示}}=0.9$, 试计算计算机系统的可靠度。

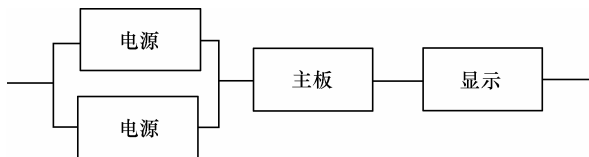


图 5-11 计算机系统可靠性框图

并联后, 电源的可靠度为: $R_{\text{电源并}} = 1 - (1 - 0.6)^2 = 0.84$, 则整个计算机的可靠度为: $R = R_{\text{电源并}} \times R_{\text{主板}} \times R_{\text{显示}} = 0.84 \times 0.9 \times 0.9 = 0.6804$ 。

3. 表决系统

表决系统是由 n 个单元组成的系统, 其中至少有任意 k 个单元正常工作, 系统就能正常工作, 称为 n 中取 k 系统。其可靠性框图见图 5-12。

利用 R_s 表示 n 中取 k 系统的可靠度, 设组成系统的 n 个单元的可靠度均为 R , 用概率法可求得 n 中取 k 系统的可靠度为:

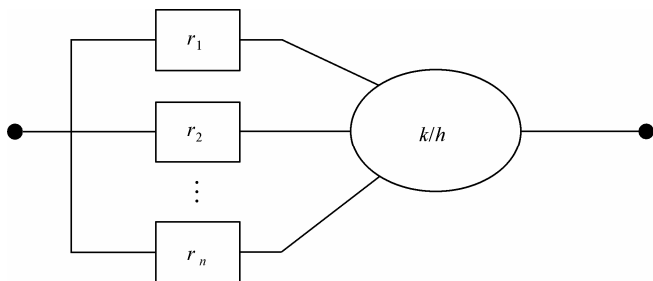


图 5-12 n 中取 k 系统可靠性框图

$$R_s = \sum_{i=k}^n \binom{n}{i} R^i (1-R)^{n-i} \quad k \leq n \quad (5-10)$$

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}$$

n 中取 k 系统是一个更为一般的可靠性模型，如果 $k=1$ ，即 n 个相同单元的并联系统；如果 $k=n$ ，即 n 个相同单元的串联系统。

4. 冷储备系统

冷储备系统或称非工作储备系统，其组成单元的可靠性不是互相独立的。冷储备系统在工作单元失效后，使非工作单元投入工作，而这个储备的非工作单元在投入工作之前是处于良好状态的。其可靠性方框图见图 5-13。

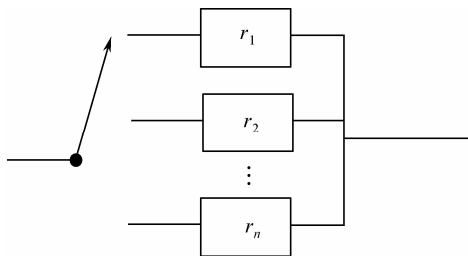


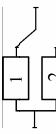
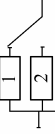
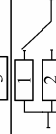

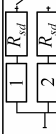
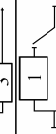
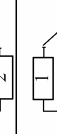

图 5-13 冷储备系统的可靠性框图

冷储备系统通常由工作单元、检测装置、自动控制开关和非工作储备单元四部分组成。当工作单元失效时，由检测装置探知、启动自动转换开关，切换至转储备单元使之投入工作。冷储备系统的可靠性分为检测装置和转换开关完全可靠，以及检测装置和转换开关具有一定可靠度时的两种情况，其计算公式列于表 5-1 中。

在表 5-1 中 R_{sd} 为检测装置和转换开关的可靠度，当其完全可靠时 $R_{sd}=1$ （在可靠性框图中可不表示），当其不完全可靠时， $0 < R_{sd} < 1$ ，在图中应标出转换开关。

从冷储备系统可靠性表达式可以看出，由指数单元组成的冷储备系统不是指数分布的。公式分为储备单元相同或不同的两种情形，公式的推导参见有关资料。

表 5-1 冷储备系统可靠性计算公式

系统类别		可靠性框图	可靠度公式	MTBF 值 (用 M_s 和 m 表示)	失效率 λ_s 公式
单元相同的冷储备系统	检测及开关装置完全可靠	2 单元		$R_S = e^{-\lambda t} (1 + \lambda t)$	$\lambda_s = \frac{1}{2} \lambda$
		3 单元		$M_S = \frac{2}{\lambda} = 2m$	$\lambda_s = \frac{1}{3} \lambda$
		n 单元		$M_S = \frac{3}{\lambda} = 3m$	$\lambda_s = \frac{1}{n} \lambda$
	检测及开关可靠度 R_{sd}	2 单元		$M_S = \frac{1}{\lambda} + \frac{R_{sd}}{\lambda}$	$\frac{1}{\lambda_s} = \frac{1}{\lambda} + \frac{R_{sd}}{\lambda}$
		3 单元		$M_S = \frac{1}{\lambda} + \frac{2R_{sd}}{\lambda} = m + 2R_{sd}m$	$\frac{1}{\lambda_s} = \frac{1}{\lambda} + \frac{2R_{sd}}{\lambda}$
单元不同的冷储备系统	检测及开关装置完全可靠	2 单元		$R_S = e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_1 + \lambda_2} (e^{-\lambda_1 t} - e^{-\lambda_2 t})$	$\frac{1}{\lambda_s} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2}$
		3 单元		$M_S = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_3} = m_1 + m_2 + m_3$	$\frac{1}{\lambda_s} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_3}$
	检测及开关可靠度 R_{sd}	2 单元		$M_S = \frac{1}{\lambda_1} + \frac{R_{sd}}{\lambda_1 - \lambda_2} (\lambda_1 - \lambda_2) (e^{-\lambda_1 t} - e^{-\lambda_2 t})$	$\frac{1}{\lambda_s} = \frac{1}{\lambda_1} + \frac{R_{sd}}{\lambda_1 - \lambda_2}$



5. 温储备系统

温储备系统的储备单元处于轻载工作状态，不处于完全不工作状态。例如，若电子管的储备单元处于不工作状态，一旦要求投入工作，由于电子管灯丝需要预热，使系统会在一段时间内中断工作。为了避免这种情况，设计时通常加上灯丝电压，有时还需要加上低于正常工作的阳极电压和假负载。这样，一旦要求投入工作，系统不会中断工作。当设备处于比较恶劣的环境时，不工作储备单元的故障率要比轻载的故障率大得多，这时也必须使储备单元处于轻载工作状态。例如，处于潮湿环境中的电子设备，通电工作的故障率要比长期储存（不工作）的故障率低。

假设单元 A 的工作故障率为 λ_A ，储备单元 B 的工作故障率为 λ_B ，轻载储备故障率为 λ'_B ，可靠性框图如图 5-14 所示。

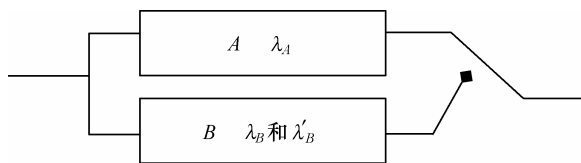


图 5-14 温储备系统的可靠性框图

可求得其可靠度和 MTBF 是：

$$R_{SW}(t) = e^{-\lambda_A t} + \frac{\lambda_A}{\lambda_A - \lambda_B + \lambda'_B} \left[e^{\lambda_B t} - e^{-(\lambda_A + \lambda'_B)t} \right] \quad (5-11)$$

当 $\lambda_A = \lambda_B = \lambda$ ， $\lambda'_B = \lambda'$ ，即工作时 A 、 B 两单元工作故障率相同时，可求得：

$$R_{SW}(t) = e^{-\lambda t} + \frac{\lambda}{\lambda'} \left[e^{\lambda t} - e^{-(\lambda + \lambda')t} \right]$$

$$\text{MTBF} = \frac{1}{\lambda} + \frac{1}{\lambda + \lambda'}$$

若检测和转换装置的故障率 λ_K 不为零或不能忽略时：

$$R_{SW}(t) = e^{-\lambda t} + \frac{\lambda}{\lambda' + \lambda_K} \left[e^{\lambda t} - e^{-(\lambda + \lambda' + \lambda_K)t} \right]$$

$$\text{MTBF} = \frac{1}{\lambda} + \frac{1}{\lambda + \lambda' + \lambda_K}$$

对于 $n-1$ 个相同的温储备单元，其可靠度和 MTBF 是：

$$R_{SW}(t) = \sum_{i=0}^{n-1} \left(\prod_{j=0, j \neq i}^{n-1} \frac{\lambda + j\lambda'}{(j-i)\lambda'} \right) e^{-(\lambda + i\lambda')t} \quad (5-12)$$

$$MTBF = \sum_{i=0}^{n-1} \frac{1}{\lambda + i\lambda'} \quad (5-13)$$

6. 循环工作的可靠性模型

在现实生活中,有许多产品,如飞机的起落架和电冰箱的压缩机,在完成任务的过程中是循环工作的。这些产品的故障率定义为循环故障率或开关故障率 λ_{cy} ,并用每个循环或每个开关动作的故障数表示。

如果 λ_{cy} 不随时间变化,那么该产品可靠度为:

$$R_C = e^{-\lambda_{cy}C} \quad (5-14)$$

式中, C 表示在完成任务过程中的循环次数。

假设在完成一项任务过程中,某产品需要循环动作 100 次,而且其故障率 $\lambda_{cy}=5$ 次故障/ 10^6 循环,则其可靠度 R_C 为:

$$R_C = e^{-5 \times 10^{-6}(100)} = 0.9995$$

如果该产品在其正常工作中为循环地接通和断开,在工作时产品的故障率为 λ_{on} ,不工作时的故障率为 λ_{off} (λ_{on} 与 λ_{off} 均用每小时的故障数表示),其循环或开关故障率为 λ_{cy} (用每个循环的故障数表示),则该产品的平均故障率 λ_{av} ,在这些条件下由下式表示:

$$\lambda_{av} = \frac{1}{t} \left[\lambda_{cy} c_f t_{cy} + \lambda_{on} t_{on} + \lambda_{off} (t - t_{cy} - t_{on}) \right] \quad (5-15)$$

式中: t ——任务时间 (h);

c_f ——循环或开关频率 (循环/h);

t_{cy} ——循环或开关过程中所占累积时间 (h);

t_{on} ——工作状态的累积时间 (h)。

则该产品的可靠度 $R(t)$ 为:

$$\begin{aligned} R(t) &= e^{-\lambda_{av}t} \\ &= e^{-[\lambda_{cy}c_f t_{cy} + \lambda_{on}t_{on} + \lambda_{off}(t - t_{cy} - t_{on})]} \end{aligned} \quad (5-16)$$

7. 串并联系统

实际的系统是多个串联、并联的组合,因此常采用串联、并联系统可靠性公式进行化简,以获得系统的可靠性表达式。在系统和整机可靠性结构确定时,其方法是采用经过由元件到组件,由组件到整机,由整机到系统这种逐级计算。为了计算

方便，也不反对将相同特点的组件、部件等在计算时进行合并。

这里的“系统”是广义的：系统对下属子系统或整机，整机对下属组件，组件对下属部件、元件等均可称为系统。这里讨论的方法，可以在各级的可靠性计算中灵活运用。

【例 5-7】串并联系统可靠性的计算

对如图 5-15 (a) 所示的系统，可化简成如图 5-15 (b) 所示的串联系统，若以小写字母代表各组件的可靠度时，化简后的 x 、 y 两个环节的可靠度表达式如下：

$$x = 2cd - c^2d^2$$

$$y = 2e - e^2$$

而这一系统的可靠度表达式为：

$$R_s = abf(2cd - c^2d^2)(2e - e^2)$$

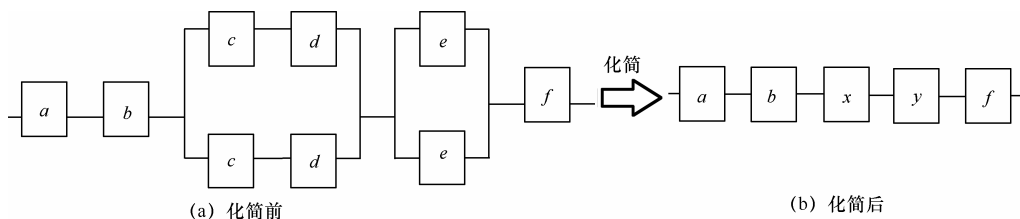


图 5-15 串并联系统可靠性框图的简化

如果各组件可靠度为已知，代入其可靠度表达式，便可算出系统的可靠度。

为便于应用，把一些简单系统可靠性公式归纳于表 5-2 中。应注意的是，表 5-2 给出的平均无故障工作时间（用 M_S ）表示及失效率 λ_S 的公式是在系统工作时间和单元工作时间相同的条件下推导出来的，推导过程这里省略了，读者若要了解可参阅相关资料。

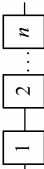
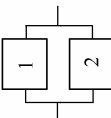
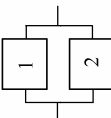
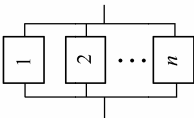

如果系统的任务时间为 t ，某单元的任务时间为 t_i ，则引入单元等效失效率：

$$\lambda_i = \frac{t_i}{t} \lambda_i' \quad (5-17)$$

式中， λ_i' 为单元失效率。

串联、并联以及串并联结合系统的可靠性模型是最为常用的，我们在表 5-2 中列出了相关的计算公式。所列公式在单元任务时间不同时，用等效失效率进行计算。这样处理后，系统和单元的任务时间都统一用系统工作时间，且可保持公式的一致性。

表 5-2 串联、并联及其组合系统可靠性计算公式

系统类别		系统通式		指数系统	
可靠性框图		可靠度公式	可靠度公式	MTBF 值 (用 M_S 和 m 表示)	失效率公式 λ_S 值
n 个单元串联系统		$R_S = r_1 r_2 \dots r_n = \prod_{i=1}^n r_i$	$R_S = e^{-\sum \lambda_{i,t}} = e^{-\lambda_S t}$	$\frac{1}{M_S} = \sum_{i=1}^n \frac{1}{m_i}$, 式中 m_i 为单元 i 的 MTBF 值	$\lambda_S = \sum_{i=1}^n \lambda_i$, 式中 λ_i 为单元 i 的失效率
		$R_S = r_1 + r_2 - r_1 r_2$	$R_S = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t}$	$M_S = m_1 + m_2 - \frac{m_1 m_2}{m_1 + m_2}$	$\frac{1}{\lambda_S} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}$
2 单元并联系统		$R_S = r_2 = r$ 时 $R_S = 2r - r^2$	$R_S = 2e^{-\lambda t} - e^{-2\lambda t}$	$M_S = \frac{3}{2} m = 1.5m$	$\lambda_S = \frac{2}{3} \lambda$
		$R_S = 1 - \prod_{i=1}^n q_i = 1 - \prod_{i=1}^n (1 - r_i)$	$R_S = 1 - \prod_{i=1}^n (1 - e^{-\lambda_{i,t}})$	$M_S = \int_0^{\infty} R_S dt$	$\lambda_S = \frac{1}{M_S}$
		各单元相同时: $R_S = 1 - (1 - r)^n$	$R_S = 1 - (1 - e^{-\lambda t})^n$	$M_S = m \left(1 + \frac{1}{2} + \dots + \frac{1}{n} \right)$	$\lambda_S = \lambda \left(\frac{1}{1 + \frac{1}{2} + \dots + \frac{1}{n}} \right)$
n 个单元并联系统		3单元相同时: $R_S = 3r - 3r^2 + r^3$	$R_S = 3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}$	$M_S = \frac{11}{6} m = 1.83m$	$\lambda_S = \frac{6}{11} \lambda$
		$R_S = (2r_1 - r_1^2)r_2 r_3$	$R_S = (2e^{-\lambda_1 t} - e^{-2\lambda_1 t}) \cdot e^{-(\lambda_2 + \lambda_3)t}$	$M_S = \frac{1}{\lambda_S}$	$\lambda_S = \frac{2}{3} \lambda_1 + \lambda_2 + \lambda_3$
串并组合系统					



5.3.8 共因故障模型

随着多通道系统使用的日益广泛，共因故障（Common Cause Failure, CCF）越来越受到人们的重视。因为这些故障一般发生在利用冗余来达到高可靠性的系统中。在这种故障状态下，一个事件或原因可使多个冗余通道同时故障并产生严重后果。事实上，大量的经验表明，这些故障不一定都具有相同的故障模式，所以目前大多数工程人员称其为共因故障。

在分析共因故障模型时，首先要明确共因故障的定义。共因故障有多种定义，但绝大多数定义都有如下共同点：

- 它们是由一个单一事件引起的。
- 该事件的结果产生多重故障。
- 这些故障往往出现在系统所确定的某些有限的时间间隔内。

简言之，共因故障就是“一个原因引起的多重故障”。值得一提的是我们应分清共因故障和系统的相关性，关于这个问题通过一个例子也许更易理解。假定在某系统中，一个电源同时供给两个或多个设备，那么电源故障就将引起所有用电设备不能工作。这不是本节所讨论的共因故障，它是系统的相关性问题，通常可直接在可靠性框图中描述。

由一个共同原因造成几个部件同时故障，这说明各故障间在统计上不是独立的，因此，当出现 CCF 时，如果我们仍按原来假定部件之间在统计上是独立的方法计算可靠性的话，所得结果必然与实际情况不符，因此有必要对其计算公式进行讨论。

现在考虑两个分别由几个相同的部件串联和并联所组成的系统。假定一个简单的数学模型，利用该模型分析 CCF 对这些系统可靠性的影响。

假设有两类事件 A 和 B 。对 A 类事件来讲，系统中的每个部件对它都是易损坏的，但该类事件将使系统中每一个部件损坏而不影响其他部件。对 B 类事件来讲，同一系统中的所有部件（同时）对它都是易损坏的，该类事件将引起所有部件同时损坏。当这两类事件 A 和 B 都出现时，其结果符合泊松过程，其故障率分别为 λ_A 及 λ_B 。

如果由于上述任一原因而造成单个部件的总故障率为 λ 的话，则： $\lambda = \lambda_A + \lambda_B$ ， $\lambda_A = (1-b)\lambda$ ， $\lambda_B = b\lambda$ 。其中 b 是 B 类事件占总事件的比例，称为共因因子。

1. 串联系统

在事件 A 、 B 存在的情况下， n 个相同部件串联，在 t 时刻系统不工作的概率为：

$$P(\text{系统不工作}) = P(\text{至少一个部件不工作})$$

$$\begin{aligned}
&= P(A \text{ 至少发生一次}) + P(B \text{ 发生}) - \text{这两项之积} \\
&= \{1 - (e^{-\lambda_A t})^n\} + \{1 - e^{-\lambda_B t}\} - \{1 - (e^{-\lambda_A t})^n\} \times \{1 - e^{-\lambda_B t}\} \\
&= 1 - e^{-(n\lambda_A + \lambda_B)t}
\end{aligned}$$

因此系统可靠度为:

$$\begin{aligned}
R_s &= 1 - P(\text{系统不工作}) \\
&= e^{-(n\lambda_A + \lambda_B)t} \\
&= e^{-\lambda t(n+b(1-n))}
\end{aligned}$$

即:

$$R_s = e^{-\lambda t n} \cdot e^{\lambda t(n-1)b} \quad (5-18)$$

① 当 $b=0$ 时, 即没有共因故障:

$$R_s(b=0) = e^{-\lambda t n}$$

这是几个故障率为 λ 的串联部件的乘积, 每个部件故障互不影响。

② 当 $b=1$ 时, 即所有故障均是共因故障:

$$R_s(b=1) = e^{-\lambda t}$$

这意味着整个系统相当于一个故障率为 λ 的部件。注意 $R_s(b=1) > R_s(b=0)$ 。

③ 对 b 取中间值, 系统可靠性比 $b=0$ 的情况提高了。我们知道 $e^{\lambda t(n-1)b} > 1$, 所以, $R_s(0 < b < 1) > R_s(b=0)$ 。

由此可见对几个部件串联的系统来讲, 当其发生共因故障时, 如果仍按部件间故障独立的方法计算可靠度的话, 计算结果要低于实际可靠度, 即过低估计了系统可靠性。

2. 并系统

在事件 A 和 B 存在的情况下, 几个相同部件并联, t 时刻系统不工作的概率为:

$$\begin{aligned}
P(\text{系统不工作}) &= P(\text{所有部件不工作}) \\
&= P(A \text{ 发生 } n \text{ 次}) + P(B \text{ 发生}) - \text{这两者之积} \\
&= (1 - e^{-\lambda_A t})^n + (1 - e^{-\lambda_B t}) - (1 - e^{-\lambda_A t})^n \bullet (1 - e^{-\lambda_B t})
\end{aligned}$$

因此系统可靠度 $R_s = 1 - P(\text{系统不工作})$, 即:

$$R_s = e^{-b\lambda t} \{1 - (1 - e^{-(1-b)\lambda t})^n\} \quad (5-19)$$

① 当 $b=0$ 时, 即无共因故障:

$$R_s(b=0) = 1 - (1 - e^{-\lambda t})^n$$

这相当于几个故障率为 λ 的相同部件并联, 每个部件独立发生故障时的情况。

② 当 $b=1$ 时, 即所有故障均是共因故障:

$$R_s(b=1) = e^{-\lambda t}$$

这正如串联那样, 系统相当于一个故障率为 λ 的部件。此时, 余度已没有价

值了。

③ 当 $0 < b < 1$ 时，共因故障的结果是此时系统的可靠度比根据假定部件故障间是独立的方法所计算的可靠度要低。这说明当出现 CCF 时，余度的作用减小了，但并不意味着余度无用了。

在上述带有 CCF 的串并联模型推导中，均假定所有的部件是相同的，实际上这是不可能的。排除这种假定需要对每个部件分别假定其独立事件的故障率 (λ_A)。

上面仅提供了一个共同原因。实际上故障原因对分析目的是不重要的，因为它们都归入共因事件 λ_B 中。然而，不同（重叠）部件组对不同的共因可能是易损的。这就增加了推导和运用概率公式的困难。然而，如果有较大影响共同原因很少，可利用马尔可夫过程来处理。

上述简单模型的讨论说明，对可靠性框图中各节点的统计独立性做出假设时应谨慎行事。因为如果假定独立，就会低估串联系统的可靠性，相反就会过高估计并联系统的可靠性。

5.3.9 多功能系统模型

对一个包括多种功能的复杂系统，或完成不同任务的可靠性命题，可分别勾画出它们的可靠性框图，同时写出各自的可靠性数学表达式，然后再根据系统的要求进行综合。

对于系统的下属组件只有一种功能者，或者各组件在时间上是相继工作的，即各组件不是同时使用的，都属于单一功能系统。

系统下属组件包括多种功能者，则属于多功能系统。下面用实例说明多功能系统可靠性的计算过程。

【例 5-8】多功能系统的可靠性计算

某一系统有两种功能，功能 I 要求组件 A 或者 B 工作，功能 II 要求组件 B 或者 C 工作，完成某一特定任务，要求功能 I、II 两种功能都正常。此系统的功能 I、功能 II 及完成任务的可靠性框图如图 5-16 所示。

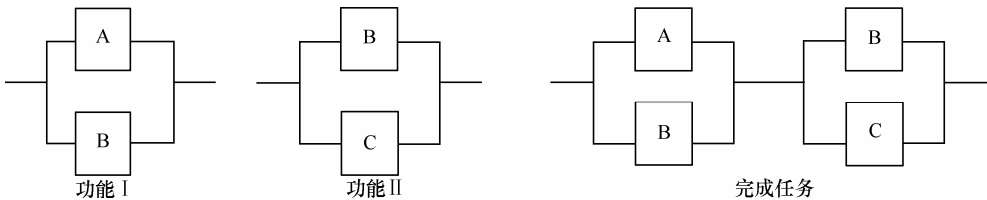


图 5-16 多功能系统的可靠性模型

假定各组件可靠度已给出： $r_a=0.9$ （组件 A）， $r_b=0.8$ （组件 B）， $r_c=0.7$ （组件 C）。

功能可靠度计算如下。

$$\text{功能 I:} \quad R_1 = r_a + r_b - r_a r_b = 0.98$$

$$\text{功能 II:} \quad R_2 = r_b + r_c - r_b r_c = 0.94$$

这里应特别注意, 系统可靠度不能用两个功能可靠度相乘的办法求出, 即系统可靠度:

$$R_s \neq 0.98 \times 0.94 = 0.9212$$

因为系统中包括多功能组件 B, 系统的可靠度表达式中有共同的 r_b , 这时应按逻辑代数的运算法则把系统可靠度表达式先化简, 再代入数值计算:

$$\begin{aligned} R_s &= (r_a + r_b - r_a r_b) (r_b + r_c - r_b r_c) \\ &= r_a r_b + r_b r_b - r_a r_b r_b + r_a r_c + r_b r_c - r_a r_b r_c - r_a r_b r_c - r_b r_b r_c + r_a r_b r_b r_c \end{aligned}$$

在逻辑代数中 $r_b r_b = r_b$, 代入上式化简得:

$$\begin{aligned} R_s &= r_b + r_a r_c - r_a r_b r_c \\ &= 0.8 + 0.9 \times 0.7 - 0.9 \times 0.8 \times 0.7 = 0.926 \end{aligned}$$

可见, 此时不能直接用简单的串并联系统的计算方法求解多功能系统的可靠度。

5.3.10 储存可靠性模型

一些产品, 如导弹和飞机的冗余部件, 从出厂到使用都要储存很长一段时间, 在任何时候, 它必须具有很高的可靠性。尤其像导弹这类产品, 经过长期储存后, 可靠性常有不同程度的降低, 甚至失效。导弹在经过一段时间的储存、检测和故障维修等状态后, 其内部材料性能的变化是导致储存可靠性下降的根本原因。由于所处的环境因素和维修管理措施的影响, 电子设备内的一些电子元件的焊接点会产生氧化膜或染上杂质; 机械零部件会产生腐蚀或生锈; 轴承用润滑油会氧化变质; 橡胶件等材料会老化变脆; 支撑结构材料微裂纹扩大等等, 这些都会导致导弹的可靠性逐渐下降。在实际使用过程中, 对导弹维修检测分为定期检测、收发检测和视情检测, 在日常采用最多的是定期检测方式。在分析计算具有储存可靠性特点的产品可靠性时, 一般需要区分以下两种情况: 一种是修复如新的情况; 另一种是修复不如新的情况。

1. 修复如新的情况

对于储存阶段的导弹, 在间隔 S 时间后进行定期检测, 对故障导弹修复后恢复至正常状态。虽然每一次修复是一次更新, 即经检测修复的导弹可靠度可以恢复到原来的水平 R_0 , 但如果是换件维修, 则新换件处于早期故障期, 故障率偏高; 如果是原件维修, 也必然使得修复后的导弹故障率增高, 即储存可靠性下降速度逐次增加。

假设导弹在出厂或开始进入使用阶段时的可靠度为 R_0 ，在不修复条件下的寿命 t 服从参数为 θ_0 的指数分布，而在第 k 次检测修复后的寿命服从参数为 θ_k 的指数分布，并且有： $\theta_0 \geq \theta_1 \geq \theta_2 \geq \dots \geq \theta_k$ 。在此条件下，假设导弹在定期检测条件下的寿命 t 的分布密度函数为指数分布：

$$f(t) = R_0 \frac{1}{\theta_k} \exp\left(-\frac{t - k\tau}{\theta_k}\right)$$

$$R(t) = R_0 \exp\left(-\frac{k - k\tau}{\theta_k}\right)$$

式中， t 为检测间隔时间， $\lambda_k = 1/\theta_k$ ，是导弹经过第 k 次检测修复后的故障率，且 k 是单调非降的。这个趋势反映了导弹储存可靠度的退化机理，假设经过第 k 次检测修复后的故障率之间的关系满足：

$$\lambda_k = \lambda_0 (k+1)^\beta$$

$$\theta_k = \theta_0 (k+1)^{-\beta}$$

式中， θ_0 为不修复条件下的平均寿命； λ_0 为固有故障率； β 为退化因子。则：

$$R(t) = R_0 \exp\{-\lambda_0 (k+1)^\beta (t - k\tau)\} \quad (5-20)$$

2. 修复不如新的情况

在长期服役过程中，导弹的一些组成部分会有缓慢的退化。而就整个导弹来讲，更换或修复的只是局部的某几个故障部件，因此，不可能达到原来的可靠度水平，由于导弹的更换件和不更换部分的共同作用，将引起定期检测间隔末端的可靠度下降。假设不更换部分的可靠度用 R_1 表示，由于不更换部分的组成非常复杂，有电子部件、机械部件、机电部件等，认为经过了老化筛选，消除了早期故障，基本控制在偶然故障阶段，可以认为是服从指数分布的复杂系统，寿命分布用下式表示：

$$R_1(t) = R_0 \exp(-\delta t)$$

式中， R_0 为导弹在出厂或开始进入使用时的可靠度； δ 为退化系数。在实际故障修复时，由于所用的备份件都是新品，可靠度视为 1，检测间隔之间的故障率随服役年限的变化不大，因此，由更换件引起的系统可靠度下降可用下式表示：

$$R_2(t) = \exp\left(-\frac{t - k\tau}{\theta}\right) = \exp\{-\lambda(t - k\tau)\}$$

$$k\tau < t \leq (k+1)\tau$$

式中， θ 为更换件的固有寿命； λ 为更换件的故障率。于是，导弹整体的可靠度函数为：

$$R(t) = R_1(t) \times R_2(t) = R_0 \exp\{-\lambda(t - k\tau) - \delta t\} \quad (5-21)$$

5.4 可靠性分配

5.4.1 可靠性分配的目的和作用

可靠性分配是为了把系统的可靠性指标按照一定的准则分配给系统各组成单元而进行的工作。其目的就是将整个系统的可靠性指标转换为每一个分系统或单元的可靠性指标,使之协调一致。它是一个由整体到局部,由上到下的分解过程。

通过可靠性指标分配,可以使各级设计人员明确其可靠性设计要求,根据要求估计所需人力、时间和资源,并研究实现这个要求的可能性及办法。如同性能指标一样,可靠性指标是设计人员在可靠性方面的一个设计目标。

可靠性分配是一个由粗到细的过程。随着研制工作的开展与深入,对系统和组成单元的认识也不不断深化、具体,应及时根据各种资料对分配的可靠性进行修正、调整。

通过可靠性指标分配,还可以暴露系统设计中的薄弱环节及关键单元和部位,为指标监控和改进措施提供根据,为管理提供所需的人力、时间和资源等信息。因而,可靠性指标分配是可靠性设计中不可缺少的工作项目,也是可靠性工程决策点。

5.4.2 可靠性分配考虑的因素

假设系统的可靠性指标可以用系统可靠度 R_s 、系统不可靠度 F_s 、系统平均无故障工作时间 $MTBF_s$ 和系统失效率 λ_s 等来表示。通过相应的分配方法来确定子系统的可靠度 R_i 、子系统故障概率 F_i 、子系统平均无故障工作时间 $MTBF_i$ 和子系统失效率 λ_i 等指标值。

在实施系统可靠性分配时,应考虑:

- 子系统复杂程度的差别。子系统包括的组件数或元件数越多,则系统越复杂。
- 子系统重要程度的差别。子系统的重要程度也称关键程度,它取决于子系统的功能与故障对系统的影响,通过对子系统的故障模式和影响分析(FMEA)可得出定性和定量的结论。重要程度用重要度来描述。
- 子系统运行环境的差别。同一系统中的各个子系统的工作环境不一定完全相同。
- 子系统任务时间的差别。一般说,对工作时间极短的子系统,其可靠度可能



达到较高的水平。

- 子系统研制周期的差别。对于个别研制周期长的单元，允许反复改进，若设计的时间较紧，在分配指标时应适当放宽。

作为一项设计，除了满足性能和可靠性指标之外，还应满足如重量、体积、成本等一些要求。因此，如何在重量、体积和成本等一些限制条件下，使产品的可靠性分配方案更为合理，也是可靠性分配要考虑的问题之一。

5.4.3 可靠性分配的原理和准则

可靠性分配问题实际上是最优化问题，因此，在分配可靠性指标时，必须明确目标函数与约束条件，基本上可分为三类：一类是以可靠性指标为约束条件，目标函数是在满足可靠性下限的条件下，使成本、质量、体积最小且研制周期尽量短；另一类是以成本为约束条件，要求可靠性尽量高；第三类是以研制周期为约束条件，要求成本尽量低，可靠性尽量高。不管是在什么情况下，都必须考虑现有技术水平能否达到所需的可靠性。所谓现有技术水平依研制周期的长短具有不同的含义。在工程计划之初到投入使用这段时间里含义也不同。对于研制周期短的产品，要提高其元器件、部件、原材料的可靠性是比较困难的，其现有技术水平就是研制初期可能达到的可靠性水平；对于研制周期长和投入使用的时间很迟的系统，现有技术水平就要考虑到交货时技术发展的水平。

系统可靠性的分配关键在于求解下面的基本不等式，即：

$$f(\hat{R}_1, \hat{R}_2, \dots, \hat{R}_n) \geq R^* \quad (5-22)$$

式中： \hat{R}_i 是给第 i 个分系统分配的可靠性参数； R^* 是系统可靠性要求参数； f 是分系统和系统可靠性间的函数关系。

从式 (5-22) 可知，可靠性分配可有无数个解，但是，所分配的可靠性指标要遵循一定的工程原则，例如，分配的指标是否能在当前的技术水平下实现？是否能够在规定的研制周期内实现？如果分配的可靠性指标，不能满足这些工程实际要求，即使分配结果能够满足系统的可靠性要求，在工程实际中也行不通，所以说，要做到既满足工程实际情况，又要在当前技术水平允许的条件下，既快又好地分配可靠性指标也不是一件很容易的事情。可靠性分配时，既要有一定的数学分析，又要有一定的工程近似，脱离工程实际纯数学分析所分配得到的可靠性指标，很可能在工程实际中实现不了。

为提高可靠性分配结果的合理性和可行性，可靠性分配应按照一定的准则进行。由于装备品种不同，工程上的问题也各式各样，在做具体可靠性分配时，可以按某一原则先计算出各级可靠性指标，然后根据以下的情况，进行一定程度的修

正；也可以在分配可靠性时，留有一定的可靠性指标余量，作为机动使用。一般应遵循的准则如下。

- 对于复杂度高的分系统、设备等，应分配较低的可靠性指标。因为产品越复杂，其组成单元就越多，要达到高可靠性就越困难，并且要花费较多的时间和费用。
- 对于重要度高的产品的可靠性指标应分配得高一些，因为关键件一旦故障，将使整个系统的功能受到影响，影响人身安全及重要任务的完成。
- 对于在恶劣环境条件下工作的分系统或部件，可靠性指标要分配得低一些，因为恶劣环境会增加产品的故障率。
- 对于新研制的、技术不太成熟的新工艺、新材料的产品，可靠性指标也应分配得低一些，因为高可靠性要求会延长研制时间，增加研制费用。
- 易于维修的分系统或部件可靠性指标可以分配得低一些，因为产品一旦出问题，则易于维修和更换。

对于已有可靠性指标的货架产品或技术成熟的系统/成品，不再参与可靠性分配。同时，在进行可靠性分配时，要从总指标中剔除这些单元的可靠性指标值。

5.4.4 可靠性分配的参数

系统可靠性分配的参数分为两类：第一类是描述系统基本可靠性的参数，常用的有：故障率 λ 、平均故障间隔时间 MTBF 等；第二类是描述系统任务可靠性的参数，常用的有：任务可靠度 R_m 、平均严重故障间隔时间 MTBCF 等。

对于不同类型的型号，描述系统可靠性的参数也不完全相同，例如对于军用飞机，可用“平均故障间隔飞行小时 (MFHBF)”描述基本可靠性指标，对于自行火炮，可用“平均使用任务中断间隔里程 (MMBOMA)”描述任务可靠性指标。

可靠性分配的指标可以是规定值，作为可靠性设计的依据；也可以是最低可接受值，作为论证的依据。在分配之前应根据实际情况给分配指标增加一定余量。

5.4.5 可靠性分配的层次

系统可靠性分配是自上而下的过程，开始于系统，终止于需要提出定量可靠性要求的产品层次。一般来说，系统可靠性分配的层次，可按下列原则确定：

- 系统中的新研产品。
- 系统中的改进产品。

特别是当上述新研或改进产品属于外协配套产品时，原则上必须分配可靠性定量要求。

5.4.6 可靠性分配的方法

1. 等分配法

等分配法又称为平均分配法，它不考虑各个单元（或元件）的重要程度，而是把系统总的可靠度平均分配给各个单元（或元件）。

在各单元的可靠度大致相同，复杂程度相差无几的情况下，用此方法最简单。它把系统看成串联系统，并设各单元的可靠度为 R_i ，则系统的可靠度 R_s 为：

$$R_s = \prod_{i=1}^n R_i \quad i=1,2,\dots,n$$

因此，组成系统的每一个单元（或元件）的可靠度为：

$$R_i = R_s^{\frac{1}{n}} \quad (5-23)$$

显然这种分配方法通常是不合理的，原因是它没有考虑到原有各分系统的可靠度，也没有考虑到各分系统的工作时间、重要性与复杂程度的差异，因此，可能会出现有的分系统可靠度根本不能达到分配的可靠度，也可能出现分配的分系统可靠度低于原有分系统的可靠度的情况。这种方法一般只在完全得不到可靠度预计数据且各组成部分可靠性差异不大的情况下才采用。

2. 考虑重要度和复杂度的分配法（AGREE 分配法）

AGREE（美国电子设备可靠性咨询组）分配法需要具有各分系统（或设备）的复杂性和重要性信息。AGREE 分配法的计算公式是：

$$R_i(t_i) = \exp\left(\frac{-t_i}{\theta_i}\right) \quad (5-24)$$

式中： $\theta_i = \frac{NW_i t_i}{n_i (-\ln R_s(t))}$ ——第 i 个分系统最低可接受的 MTBF 值；

$N = \sum_{i=1}^n n_i$ ——系统中的组装件（软件中称之为模块）总数；

n_i ——第 i 个分系统的组装件数目；

t ——规定的系统任务时间；

t_i ——规定的第 i 个分系统的任务时间；

W_i ——重要性因子，用第 i 个分系统发生故障将会导致系统故障的概率表示；

$R_s(t)$ ——在系统任务时间内要求的系统可靠度。

3. ARINC 分配法

ARINC 分配法适用于故障率恒定的串联分系统，任一分系统发生故障都会使整个系统发生故障，而且各分系统的任务时间与系统任务时间相等。

计算公式：

$$\lambda_i^* = w_i \lambda^*$$

式中： $w_i = \frac{\lambda_i}{\sum_{i=1}^n \lambda_i}$ （加权因子）；

n ——下一层次组成的单元数；

λ^* ——要求的系统失效率；

λ_i ——单元 i 的失效率；

λ_i^* ——分配到单元 i 的失效率要求。

4. 评分分配法（目标可行性法）

评分分配法又称“目标可行性法”或“综合因子法”。评分分配法是通过影响产品可靠性的几种因素评分，并对评分值进行综合分析以获得各单元产品之间的可靠性相对比值——分配系数，再根据分配系数给每个单元产品的可靠性指标进行分配的方法。

评分分配法的计算公式：

$$\lambda_i = C_i \lambda_s \quad (5-25)$$

式中： $C_i = \frac{w_i}{w}$ （分系统 i 的归一化因子）；

$W_i = \prod_{j=1}^m \gamma_{ij}$ （分系统 i 的因子之积）；

$W = \sum_{i=1}^n W_i$ ；

N ——分系统数目；

λ_s ——要求的系统失效率；

λ_i ——分配给分系统 i 的失效率；

γ_{ij} ——分系统 i 的第 j 个因子；

M ——考虑因素的数目。

评分分配法通常考虑的评分因素有：复杂程度、技术成熟水平、工作时间、环境条件等。根据系统的特点可以增加或减少评分因素。评分准则是评分的依据，以下给出常用因素的评分准则，包括评价分数及范围，以及各分值的说明，其分值越高说明可靠性越差。



- 系统复杂程度：可根据被评价产品的元部件数量以及它们组装的难易程度来评定。表 5-3 给出一种推荐的复杂程度因素评分准则。
- 技术成熟水平：根据被评产品的技术水平和成熟程度进行评定。表 5-4 给出一种推荐的技术成熟水平因素评分准则。
- 工作时间：根据被评产品的工作时间进行评定。表 5-5 给出一种推荐的工作时间因素评分准则。
- 环境条件：根据被评产品所处的环境进行评定。表 5-6 给出一种推荐的环境条件因素评分准则。

其他因素的评分原则和依据，可根据系统特点以及对系统可靠性的影响程度来确定。

表 5-3 复杂程度因素评分准则

等 级	分 数	说 明
1	9~10	该单元产品的元部件数量（组装时间）是所有同级组成单元产品最大数量（最长组装时间）的 80%~100%
2	7~8	该单元产品的元部件数量（组装时间）是所有同级组成单元产品最大数量（最长组装时间）的 60%~80%
3	5~6	该单元产品的元部件数量（组装时间）是所有同级组成单元产品最大数量（最长组装时间）的 40%~60%
4	3~4	该单元产品的元部件数量（组装时间）是所有同级组成单元产品最大数量（最长组装时间）的 20%~40%
5	1~2	该单元产品的元部件数量（组装时间）是所有同级组成单元产品最大数量（最长组装时间）的 20%以下

表 5-4 技术成熟水平因素评分准则

等级	分 数	说 明
1	9~10	掌握技术的基本原理或明确技术概念及如何应用
2	7~8	已进行概念验证、主要功能的分析和验证，或已在实验室环境中验证主要功能模块
3	5~6	已在相似环境中验证主要功能模块，或已在相似环境中验证系统及原型
4	3~4	已在运行环境中验证原型，或实际系统已通过试验和验证
5	1~2	实际系统已成功应用

表 5-5 工作时间因素评分准则

等级	分 数	说 明
1	9~10	该单元产品的工作时间是同级单元产品最长工作时间的 80%~100%
2	7~8	该单元产品的工作时间是同级单元产品最长工作时间的 60%~80%

(续表)

等级	分 数	说 明
3	5~6	该单元产品的工作时间是同级单元产品最长工作时间的 40%~60%
4	3~4	该单元产品的工作时间是同级单元产品最长工作时间的 20%~40%
5	1~2	该单元产品的工作时间是同级单元产品最长工作时间的 20% 以下

表 5-6 环境条件因素评分准则

等级	分 数	说 明
1	9~10	该单元产品处于系统中最恶劣的工作环境之中（如工作温度最高、振动加速度最大、湿度最大等）
2	7~8	该单元产品处于系统中较恶劣的工作环境之中（如工作温度较高、振动加速度较大、湿度较大等）
3	5~6	该单元产品处于系统中适中的工作环境之中（如工作温度适中、振动加速度适中、湿度适中等）
4	3~4	该单元产品处于系统中较好的工作环境之中（如工作温度适中、振动加速度较小、湿度较小等）
5	1~2	该单元产品处于系统中最好的工作环境之中（如工作温度适宜、振动加速度最小、湿度最低等）

5. 比例组合分配法

比例组合分配法是根据相似老系统中各单元产品的故障率或单元产品预计数据进行分配的一种方法。比例组合分配法可以对系统的故障率、MTBF 等基本可靠性指标进行分配。

如果一个新设计的系统与老的系统非常相似，也就是组成系统的各单元类型相同，对这个新系统只是提出新的可靠性要求，那么，就可以采用比例组合法。根据老系统中各单元的故障率，按新系统可靠性的要求，给新系统的各单元分配故障率。这种方法认为原有系统基本上反映了一定时期内产品能实现的可靠性，新系统如果有个别单元在技术上有什么重大的突破，那么按照现实水平，可把新的可靠性指标按其原有能力成比例地进行调整。这种方法只适用于新、老系统结构相似，而且有老系统统计数据或是在已有各组成单元预计数据基础上进行分配的情况。

在应用比例组合分配方法时，需要注意：

- 该方法只能在新、老系统功能、结构、使用环境相似的条件下应用。
- 老系统各单元产品故障率可以获取。

比例组合分配法的数学表达式为：

$$\lambda_{i\text{新}}^* = \lambda_{s\text{新}}^* \cdot \frac{\lambda_{i\text{老}}}{\lambda_{s\text{老}}} \quad (5-26)$$

式中： $\lambda_{s\text{新}}^*$ ——新系统的故障率指标；

$\lambda_{i\text{新}}^*$ ——分配给新系统中第 i 个单元的故障率；



$\lambda_{s老}$ ——老系统的故障率；

$\lambda_{i老}$ ——老系统中第 i 个单元的故障率。

如果有老系统中各分系统故障数占系统故障数百分比 K_i 的统计资料，那么可以按式 (5-27) 进行分配：

$$\lambda_{i新}^* = \lambda_{s新}^* \cdot K_i \quad (5-27)$$

式中， K_i 为第 i 个分系统故障数占系统故障数的百分比。

6. 最少工作量法（可靠度再分配法）

这种方法考虑使系统可靠性要求的总工作量最少。假设系统由 n 个分系统串联组成，并假定每个分系统的可靠度是在现有的研制阶段进行度量或估算的，并进行可靠性分配使得可靠度较低的分系统有较大的提高。

设 R_1, R_2, \dots, R_n 表示各分系统的可靠度，系统的可靠度 R 由下式给出：

$$R = \prod_{i=1}^n R_i \quad (5-28)$$

设 R^* 为要求的系统可靠度，且 $R^* > R$ 。接着，至少需要将一个 R_i 值提高到可使要求的可靠度 R^* 得到满足的程度。为了提高某些分系统的可靠度，需要花费一定的工作量，这些工作量必须由各分系统分摊。这些工作量将是试验数、工程人员数量等的函数。

这种方法假设每一个分系统具有相同的工作量函数 $G(R_i, R_i^*)$ ，该函数是将第 i 个分系统的可靠度从 R_i 提高到 R_i^* 所需工作量的度量。

7. 直接寻查法

直接寻查法是在已知各单元可靠度、各单元所占用资源数量的条件下，计算满足系统要求各资源最大值的情况下，各单元的冗余数量。应用直接寻查法进行可靠性分配时，需要输入系统各资源的最大值、各单元可靠度以及占用资源数量。

8. 拉格朗日乘数法

该方法的思路是建立一个拉格朗日函数，使它包含可靠性目标函数、约束条件函数。然后，将有约束条件求极值问题转化为无约束条件求极值问题。

假设某系统包含的等效串联分系统数为 n ，则拉格朗日函数 $L(K_i, \lambda)$ 的表达式为：

$$L(K_i, \lambda) = \prod_{i=1}^n (1 - F_i^{k_i}) + \lambda \left(W_0 - \sum_{i=1}^n W_i K_i \right) \quad (5-29)$$

式中： K_i ——第 i 个等效串联分系统中，并联单元数；

F_i ——第 i 个等效串联分系统中，单个单元的不可靠度；

W_o ——系统的约束条件，例如系统的成本、质量等；

W_i ——第 i 个等效串联分系统中，单个单元的成本、质量等；

λ ——拉格朗日乘数。

在给定的特定条件下：

$$\frac{\ln F_i}{W_i} = C(\text{常数})$$

对 $L(k_i, \lambda)$ 取偏导数求极值，经数学运算后可求得约束条件下的最佳并联单元数：

$$K_i = \frac{W_o}{\ln F_i} / \sum_{i=1}^n \frac{W_i}{\ln F_i} \quad (5-30)$$

$\frac{\ln F_i}{W_i} = C(\text{常数})$ 意味着每一个单元不可靠度的对数与其成本（或质量等）之比

为固定比例，也就是说，愈可靠的单元其成本愈高（或质量愈重），这在实际应用中还是有一定的运用范围。

9. 基于遗传算法的可靠性分配方法

对于通信网络系统或者网状结构的复杂系统来说，或者是建立的可靠性模型复杂，且很难采用串联、并联等关系描述时，需要采用基于遗传算法等优化方法进行可靠性分配。

以如图 5-17 所示的复杂系统为例，假设该系统的总费用不超过 $C_{s \max}$ ，系统可靠性指标最低为 $R_{s \min}$ ，各部件（图中的 1、2、3、4）的价格模型为：

$$C_i = K_i R_i^{a_i} \quad (5-31)$$

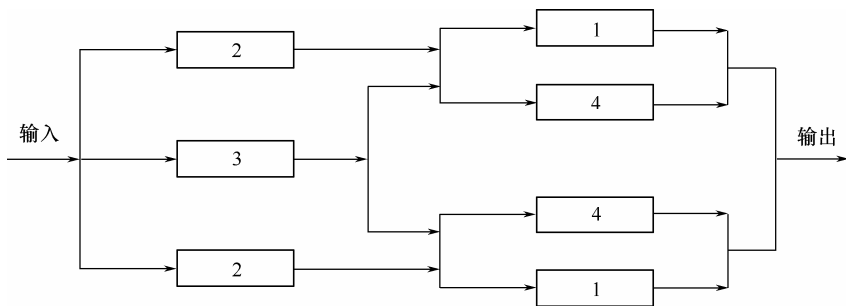


图 5-17 某系统可靠性框图

C_i 为第 i 个部件费用， K_i 、 a_i 是与部件结构有关的参数， $a_i \leq 1$ 。令 Q_s 为系统失效概率（或不可靠度）， R_s 为系统可靠度， Q_i 为部件 i 的失效概率（或不可靠

度), R_i 为部件 i 的可靠度。经推导, 系统失效概率为:

$$Q_s = (Q_1Q_4)^2 R_3 + (Q_2 + R_2Q_1Q_4)^2 Q_3 \tag{5-32}$$

当 K_i 、 a_i 已知 ($K_1=100$, $K_2=100$, $K_3=200$, $K_4=150$, $a_i=0.6$), $C_{s\max}=800$, $R_{s\min}=0.99$, $R_{i\min}=0.5$ 的情况下, 如果要分配系统的可靠性时应如何分配?

从图 5-17 以看出, 该系统的可靠性框图, 很难采用串联、并联或者表决等关系描述。对于简单的并一串、串一并冗余结构, 一般可以采用解析方法给出可靠性计算和分配方案, 但像图 5-18 这样比较复杂的系统, 首先需根据其结构推出可靠性计算公式, 并采用非线性最优化方法 (如遗传算法) 求解, 以确定各个部件的可靠度。遗传算法是一种多目标优化方法, 其在解决多目标、多资源约束条件下的优化方面具有优势。

10. 考虑置信度的可靠性分配

进行系统可靠性分配, 目的就是将整个系统的可靠性指标转换为每一个分系统或单元的可靠性指标, 使之协调一致。由于系统的复杂性, 组成系统的分系统、单元较多, 如果在可靠性分配过程中, 不考虑各分系统、单元的可靠性指标的置信水平, 直接根据可靠性分配的指标值进行各分系统、单元的设计, 在后期试验验证、评价过程中, 可能会出现系统可靠性指标不达到预期的后果, 所以, 在实际进行可靠性分配过程中, 需要考虑分配的各分系统、单元的可靠性指标的置信度水平。

5.4.7 不同研制阶段可靠性分配方法的选择

要进行可靠性分配, 首先必须明确设计目标、限制条件、系统下属各级定义的清晰程度, 以及有关类似产品可靠性数据等信息。随着研制阶段的进展, 则可靠性分配也有所不同, 如表 5-7 所示。

表 5-7 不同研制阶段可靠性分配方法的选择

研制阶段	可靠性分配方法
方案阶段	等分配法、ARINC 分配法等
初步设计	评分分配法、比例分配法、最小工作量法等
详细设计	考虑重要度和复杂度分配法, 最小工作量法, 拉格朗日待定系数法等

5.4.8 进行可靠性分配时的注意事项

进行可靠性分配工作时, 需要注意以下几点:

- 可靠性分配应在研制阶段的早期开始进行，这样可以：
 - ◆ 使设计人员尽早明确其设计要求，研究实现这个要求的可能性。
 - ◆ 为外购件及外协件提出可靠性指标提供初步依据。
 - ◆ 根据所分配的可靠性要求估算所需人力和资源等管理信息。
- 可靠性分配应反复多次进行。在方案论证和初步设计工作中，分配是较粗略的，仅粗略分配后，应与经验数据进行比较、权衡；也可和不依赖于初步分配的可靠性预测结果相比较，确定分配的合理性，并根据需要重新分配。随着设计工作的不断深入，可靠性模型逐步细化，可靠性预计工作亦须随之反复进行。
- 为了尽可能减少可靠性分配的重复次数，在规定可靠性指标的基础上，可考虑留出一定的余量。这种做法为在设计过程中增加新功能元件留下了考虑的余地，因而可以避免为适应附加的设计而必须反复分配。
- 可靠性分配的主要目的是使各级设计人员明确其可靠性设计目标，因此，必须按成熟期规定值（或目标值）进行分配。
- 可靠性分配时，可考虑分配的指标置信度。

5.5 可靠性预计

可靠性预计是指为了估计产品在给定工作条件下的可靠性而进行的工作。

在新系统的设计阶段就要对系统的可靠性进行预计，以便及时发现设计中存在的可靠性方面的问题并及时修改，确保在费用和时间等资源限制下达到要求的指标。

显然，系统的可靠性预计实质是在系统的设计阶段根据组成系统的元器件等，在规定工作条件下的可靠性指标、系统的结构、系统的功能以及工作方式等来推测系统的可靠性，这是一个由局部到整体、由小到大、由下到上的一种预测方法。而可靠性分配是从系统直到最低单元的由上而下的分配过程。二者往往交互进行，它也是可靠性设计的重要内容之一。

5.5.1 可靠性预计的目的和作用

1. 可靠性预计的目的

- 将预计结果与要求的可靠性指标相比较，审查设计任务书中提出的可靠性指标是否能达到。
- 在方案论证阶段，通过可靠性预计，根据预计结果的相对性进行方案比较，



选择最优方案。

- 在设计阶段，通过预计，发现设计中的薄弱环节及存在问题，及时采取改进措施，加以改进。
- 为可靠性增长试验、可靠性鉴定试验、可靠性验收试验及费用核算等方面的研究提供依据。
- 通过预计给可靠性分配奠定基础。

可靠性预计的主要价值在于，它可以作为设计手段，为设计决策提供依据，因此，要求预计工作具有及时性，即在决策之前做出预计，提供有用的信息，否则这项工作就会失去其意义。为了达到预计的及时性，在设计的不同阶段及系统的不同级别上可采用不同的预计方法，由粗到细，随着研制工作的深化而不断细化。

在可靠性设计过程中，预计与修改设计是交替进行的，发现问题要及时修改。经验证明，修改越及时，研制周期越短，越经济。可以说可靠性预计和修改的过程就是可靠性增长的过程。

2. 可靠性预计的作用

- 在设备、系统的设计阶段，定量地预测其可靠性水平，评价电子设备、系统是否能达到要求的可靠性指标。例如某电能表的招标书中规定：产品的设计寿命为 15 年，要求 15 年内其累计故障率不超过 10%。按指数分布推算，其平均故障间隔时间要大于 140 年才能满足要求，此时，只有对设计阶段的产品进行可靠性预计，才能判断其是否满足指标要求，才能为中标提供技术保证。
- 通过可靠性预计为可靠性分配奠定基础，并为拟定改正措施的优先顺序提供依据，将产品可靠性指标自上而下逐级地分配给产品的各个层次，借此落实相应层次的可靠性要求，并使整体与各部分之间的可靠性相互协调，尽可能地做到既避免出现薄弱环节，又避免局部“质量过剩”而带来浪费。可靠性预计结果为实施可靠性分配提供了直接定量的依据。
- 在方案论证阶段，通过可靠性预计，可对不同方案的可靠性水平进行比较，指导元器件的合理选用，为最优方案的选择及方案优化提供依据。可靠性预计手册中给出了各类别元器件的质量等级及其质量系数，也给出了执行不同生产标准的产品失效率之间的差别，何种等级的元器件易引发高故障率，这就为合理选用元器件提供了依据。为满足工程对可靠性的高要求，设备研制单位选用高质量的元器件，可促进元器件生产厂家的技术改造、新品开发、军标实施等工作，促进元器件的可靠性上新台阶。
- 在设计中，通过可靠性预计，发现影响电子设备可靠性的主要因素，从而及时改进设计，实现产品的高可靠性。
- 对已投入现场使用的设备、系统进行可靠性预计，为合理制订储备与更新计

划提供依据；通过对现场使用的设备、系统进行可靠性预计，确定产品的薄弱环节，对可靠性较低的产品及时做好储备或更新，以保障设备和系统的正常工作。

- 为可靠性增长计划提供信息，为可靠性增长试验、验证试验及费用核算等研究提供依据。
- 通过可靠性预计与失效模式及影响分析，鉴别可靠性薄弱环节，为维修、后勤保障方案提供依据。

5.5.2 可靠性预计的内容

可靠性预计按不同的目的和要求有不同的内容。

1. 按预计指标的不同分为基本可靠性预计和任务可靠性预计

基本可靠性预计可以表明由于产品的不可靠，给维修和保障所增加的负担；而任务可靠性预计是预计产品成功完成规定任务的能力，以便为产品的作战效能分析提供依据。两者应结合进行，一般在产品设计的早期阶段，任务可靠性预计往往难以进行，此时一般做必要的基本可靠性预计。随着设计工作的深入开展，两种预计可逐步同时进行，其预计结果可以为设计人员提供权衡设计的依据。通过预计，若基本可靠性不足，可采用简化设计，使用高质量元器件或采用冗余方法来解决。

2. 按预计时间的不同分为方案论证阶段和工程设计阶段的预计

方案论证阶段预计的任务是估计各设计方案满足可靠性指标的可能性，主要估计 MTBF 和 MTTR，这对于从几种竞争的备选方案中选择最优方案有重要作用，对节省研究时间和经费也有重要的作用，因此越来越被重视。设计阶段预计的任务是估计具体设计的可靠性。在设计的前期、中期和最后三个阶段要分别进行可靠性预计。初期的预计是根据初期的设计草图进行的，边预计边修改。因此，它只能大概地预示系统最后可能达到的可靠性水平。中期的预计能验证实现初期预计的程度，并预示最后能达到的可靠性水平。由于设计资料的增加（如环境数据和内部负载等资料），因此，它比初期的预计精度提高了。最后的预计是根据设计的最后阶段的系统进行的，它是根据全部设计过程的资料预计的，因此它能较好地预示系统可能达到的可靠性。

5.5.3 系统可靠性预计方法

在工程上可靠性预计，常用的方法有：元器件计数法、应力分析法、相似产品法、故障率预计法、专家评分法、相似产品类比论证法、可靠性框图法、功能预计

法、上下限法等。

1. 元器件计数法

该方法适用于电子类产品的基本可靠性预计，主要用于方案论证及初步设计阶段。这种方法是以前元器件的可靠性数据为基础预计系统的可靠性。元器件的可靠性数据是不能用计算方法得出的，只能在实际的工作场合或在实验室中测出，而且大多数的零部件或元器件，都是假定失效分布类型为指数分布，由于指数分布的失效率 λ 是一常数，因此，在进行预测计算时就方便得多。目前，有些国家采用寿命试验的方法，求出各种元器件的失效率数据，编成手册，以供使用，例如，GJB/Z 299C《电子设备可靠性预计手册》。在元器件计数法中，元器件的质量系数、通用失效率等都可从手册中查出。

元器件计数法用于初步设计阶段，这时已大致知道将用于某设备的各种等级和类型（电阻器、电容器、变压器）的元器件数目，不需要知道每个元器件的工作应力。这种方法所需的信息为：每一类型的元器件数目，该类元器件的通用失效率和质量水平，以及设备的环境条件。

元器件计数法预计设备失效率的数学模型为：

$$\lambda_s = \sum_{i=1}^n N_i (\lambda_{Gi}, \pi_{Qi}) \quad (5-33)$$

式中： λ_s ——设备的总失效率，它反映了在设计制造和试验过程中，工艺质量控制等级，一般可分为 A、B、C 三级，可查专用表；

λ_{Gi} ——第 i 个元器件的通用失效率；

π_{Qi} ——第 i 个元器件的质量系数；

N_i ——第 i 个元器件的数量；

N ——不同的元器件种类的数目。

通用失效率是指电子元器件在不同环境中，在通用工作环境温度 and 常用工作应力条件下的失效率，通用工作环境温度是指在不同环境条件下，各类器件在工作时通用的周围环境温度。

若设备是在同一环境工作，则可直接使用上述表达式。如果设备是由几个单元组成的，而且各单元的工作环境也不同（例如，机载武器系统由几个单元组成，其中有些单元处于舱内，有些单元则可能悬挂在机舱外），则应该按每一环境中的单元工作失效率计算公式计算（公式可参考 GJB/Z 299C《电子设备可靠性预计手册》），然后将这些单元的工作失效率相加，求出设备总失效率。其中环境系数可查 GJB/Z 299C。

应用元器件计数可靠性预计法较简便，以基于 GJB/Z 299C 的预计手册进行可

靠性预计为例，说明其基本程序为：

- ① 列出设备所用的元器件种类以及每类元器件的数量、质量等级和设备的应用环境类别。
- ② 从 GJB/Z 299C 的第 6 章，查得各种类元器件在该环境类别下的通用失效率 λ_G ，以及通用质量系数 π_Q 。
- ③ 将①、②步骤所得到的数据填入失效率预计表，如表 5-8 所示。

表 5-8 失效率预计表（样式）

项目名称：					组件名称：			MTBF：	
阶段：		工作状态：			Σ数量：			Σ失效率：	
序号/节点名称/ 位号	型号	类别	环境	质量 等级	质量系数 π_Q	数量	λ_G (10 ⁻⁶ /h)	$\lambda_G\pi_Q$ (10 ⁻⁶ /h)	$N\lambda_G\pi_Q$ (10 ⁻⁶ /h)

- ④ 按式（5-33）分别计算不同应用环境下的分系统或单元失效率。
- ⑤ 将分系统或单元失效率按可靠性模型及对应的数学表达式进行计算，获得整个系统、设备的总失效率及其 MTBF 等可靠性指标。

2. 应力分析法

应力分析法适用于电子类产品在详细设计阶段的可靠性预计，它是以每一类型元器件的质量水平、工作应力及环境应力等因素以及每一类型元器件的平均失效率为基础进行分析，但是元器件的强度与元器件应力水平之间的相互关系，决定了在给定条件下的元器件失效率。因此，元器件处于不同的应力水平就会有不同失效率，这就是应力分析法的原理。应力分析法需要知道元器件所承受的应力，如温度、湿度、振动等，这就决定了这种方法只能在详细设计阶段进行。该方法与元器件计数法的不同之处，就是根据元器件所处的实际应力环境条件，对元器件的失效率进行修正。这种方法首先建立元器件失效率模型（可查《电子设备可靠性预计手册》），根据所给的环境应力，就能算出元器件的工作失效率，然后根据可靠性框图的逻辑关系，计算出设备的总失效率。

下面介绍元器件应力分析可靠性预计法的一般程序。

在获得元器件工作失效率预计模型相应的数据、信息之后，可按下述步骤有条不紊地逐级进行预计：

- ① 参照设备、系统的功能原理，划分除在电路功能上相对独立、内部为串联结构的可靠性预计单元，然后确定各预计单元间的可靠性逻辑关系和数学关系，即

建立产品可靠性模型。

② 分析各元器件的应用方式、工作环境温度及其他环境应力，以及电应力比等工作应力数据。

③ 汇编设备的元器件详细清单，清单内容包括：元器件名称、型号规格、数量、产品标准或技术文件、性能额定值，以及有关的设计、工艺、结构参数和工作应力数据等。

④ 按照各种类元器件的工作失效率模型，计算每个预计单元内各元器件的工作失效率。

⑤ 将②～④步骤所得到的数据填入规范化的预计表内，如表 5-9 所示。

表 5-9 应力分析可靠性预计法预计表（样式）

项目名称:			组件名称:						MTBF:		
阶段:			工作状态:				Σ数量:		Σ失效率:		
序号/节点名称/位号	型号	类别	预计依据	环境	温度(℃)	质量等级	应力比	π 系数	数量	失效率(10 ⁻⁶ /h)	失效率分布

⑥ 将预计单元内元器件的工作失效率相加，由此计算组件或分系统的失效率。

⑦ 按设备、系统的可靠性模型，逐级预计设备、系统的平均故障间隔时间与可靠度等可靠性指标。

一般产品的元器件数量较多，如果利用应力分析法预计其可靠度是很烦琐且费时的。目前，国内外已开发了相关软件工具，利用计算机辅助预计软件工具进行可靠性预计，可大大节省人力和时间。

3. 相似产品法

相似产品法适用于机械、电子、机电类产品等具有相似可靠性数据的新产品在方案论证及初步设计阶段的可靠性预计。它适用于初始构思、规划新品方案的总体论证阶段，由于信息少，只能大体估计，通过一些简单的预计，如寻求在用途、性能和结构等方面与研制进行对象相类似的老产品或电路，以其可靠性水平作为所研制产品可靠性的估计值。借此对新品可能达到的可靠性水平进行粗略的预测，进而评估新品总体方案的可行性。

该方法的适用条件对新设备与老设备是相似的，以及老设备的可靠性水平是已知的。相似法的预计精度取决于现有设备可靠性数据的可信程度，以及现有设备和新设备的相似程度。

（1）相似产品法考虑的相似因素

- 产品结构、性能的相似性。

- 设计的相似性。
- 材料和制造工艺的相似性。
- 使用剖面（保障、使用和环境条件）的相似性。

这种方法简单、快捷，适用于系统研制的各个阶段，可应用于各类产品的可靠性预计，如电子、机械、机电等产品，其预计的准确性取决于产品的相似性。成熟产品的详细故障记录越全，数据越丰富，新老产品比较的基础越好，预计的准确度越高。

（2）相似产品法的预计程序

- 确定相似产品。考虑前述的相似因素，选择确定与新产品最为相似，且有可靠性数据的产品。
- 分析相似因素对可靠性的影响。分析所考虑的各种因素对产品可靠性的影响程度，分析新产品与老产品的设计差异以及这些差异对可靠性的影响。
- 新产品可靠性预计。确定新产品与老产品的可靠度比值，当然，这些比值应由有经验的专家评定。最终，根据比值预计出新产品的可靠度。

4. 故障率预计法

当系统进展到详细设计阶段，既有系统原理图和结构图，也选出了元器件，并且已知元器件的类型、数量、环境及使用应力，具有实验室常温条件下测得的故障率时，可用故障率预计法进行系统可靠性预计。故障率预计法可用于机械、电子、机电类产品的可靠性预计，其原理与电子产品应力分析法基本相同。但要求组成产品的所有单元、元器件均有故障率数据。故障率预计法是将元部件的故障率代入所需预测的系统的可靠性数学模型中进行计算，从而得到系统可靠性预测值。

目前，在设计阶段都要用这种方法进行较精确的预计。大多数情况下，获得的元件故障率是常数，是在实验室条件下测得的数据，叫作“基本故障率”，用 λ_b 表示。但在实际应用中，必须考虑环境条件和应力状况，将基本故障率转化成应用条件下的故障率，用 λ 表示。

因此，要正确地应用故障率预计方法进行可靠性预计，需要具备下列 3 个条件：已知所预测系统的原理图、详细设计图、结构图；能够建立其可靠性数学模型；已知设备所用的各种元部件的类型、数量、环境及使用应力，以及在实验室常温条件下测得的“基本故障率”等数据。如果具备上述 3 个条件，即可应用故障率预计法进行可靠性预计，故障率预计方法的一般步骤如下：

- ① 明确预计的内容、范围和指标。
- ② 正确地建立系统的可靠性数学模型。
- ③ 列举出全部元部件清单，并注明规格、数量、特殊的工作条件、使用环

境、故障率等。

④ 考虑和分析机械零件的应力和强度，确定适当的安全系数。

⑤ 计算系统的故障率 $\lambda_s(t)$ 。 $\lambda_s = \lambda_b \cdot \pi_E \cdot D$ 。 λ_s 为工作故障率； λ_b 为基本故障率； π_E 为环境因子，可查 GJB/Z 299C 等手册获得； D 为由工程经验取值的降额因子，取值为 0~1。

⑥ 计算系统的可靠度 $R(t) = \exp[-\lambda_s(t)t]$ 。

⑦ 计算系统的平均寿命 $T_{BF} = 1/\lambda_s$ 。

⑧ 判断系统的可靠性指标是否达到了要求。

若能满足要求，则不必用昂贵的元器件，不必采取特殊措施，就可以降低成本，节省时间；若未达到要求，则应改用更可靠的元器件等，或采用其他方法来提高系统的可靠性，如降额设计、降温设计、冗余设计等。

5. 专家评分法

专家评分法适用于机械、机电类产品，产品中仅有个别单元的故障率数据，用于产品的方案论证及初样设计与正样设计阶段中。

专家评分法是依靠有经验专家的工程经验，按照几种因素进行评分。按评分结果，由已知的某单元故障率数据，根据评分系数，算出其余单元的故障率。

(1) 评分考虑的因素

评分考虑的因素可按产品特点而定。这里介绍以产品故障率为预计参数说明常用的 4 种评分因素，每种因素的分数为 1~10 分。

- 复杂度。它是根据组成成分系统的元、部件数量，以及它们组装的难易程度来评定，最简单的评 1 分，最复杂的评 10 分。
- 技术水平。根据分系统目前的技术水平和成熟性来评定，水平最低的评 10 分，水平最高的评 1 分。
- 工作时间。根据分系统工作时间来评定。系统工作时，分系统一直工作的评 10 分，工作时间最短的评 1 分。
- 环境条件。根据分系统所处的环境来评定，分系统工作过程中会经受极其恶劣和严酷的环境条件的评 10 分，环境条件最好的评 1 分。

(2) 专家评分法的实施

已知某一分系统的故障率为 λ^* ，算出的其他分系统故障率为：

$$\lambda_i = \lambda^* \cdot C_i \quad (5-34)$$

式中： i ——分系统数， $i=1, 2, \dots, n$ ；

C_i ——第 i 个分系统的评分系数。

$$C_i = \omega_i / \omega^*$$

$$\omega_i = \prod_{j=1}^4 r_{ij}$$

式中： r_{ij} 表示第 i 个分系统，第 j 个因素的评分数， $j=1$ 时表示复杂度； $j=2$ 时表示技术水平； $j=3$ 时表示工作时间； $j=4$ 时表示环境条件。

【例 5-9】利用专家评分法进行可靠性预计

某飞行器由动力装置、武器等 6 个分系统组成（如表 5-10 所示）。已知制导装置故障率为 $284.5 \times 10^{-8}/\text{h}$ ，即 $\lambda^* = 284.5 \times 10^{-8}/\text{h}$ ，试用评分法求其他分系统的故障率，一般计算可用表格进行。

表 5-10 某飞行器的故障率计算

序号	分系统名称	复杂度 r_i	技术水平 r_{i2}	工作时间 r_{i3}	环境条件 r_{i4}	分系统评分分数 ω_i	分系统评分分数 $C_i = \omega_i / \omega^*$	各分系统的故障率/ ($\times 10^{-8}/\text{h}$) $\lambda_i = \lambda^* \cdot C_i$
1	动力装置	5	6	5	5	750	0.300	85.4
2	武器	7	6	10	2	840	0.336	95.6
3	制导装置	10	10	5	5	(ω^*) 2500	1.0	(λ^*) 285.4
4	飞行控制装置	8	8	5	7	2240	0.896	254.9
5	机体	4	2	10	8	640	0.256	72.8
6	辅助动力装置	6	5	5	5	750	0.3	85.4

表 5-10 中最右列即根据专家评分法计算得到的各分系统故障率。把该列数值相加，即得该飞行器故障率 $878.6 \times 10^{-6}/\text{h}$ 。

6. 相似产品类比论证法

相似产品类比论证法是机械产品可靠性预计方法。其基本思想是根据仿制或改型的类似国内外产品已知的故障率，分析两者在组成结构、使用环境、原材料、元器件水平、制造工艺水平等方面的差异，通过专家评分给出各修正系数，权衡后得出一个故障率综合修正因子，即：

$$D = K_1 \cdot K_2 \cdot K_3 \cdot K_4 \cdot K_5 \quad (5-35)$$

式中： D ——故障率综合修正因子；

K_1 ——原材料水平与先进国家原材料的差距的修正系数；

K_2 ——基础工业（包括热处理，表面处理、铸造质量控制等方面）与先进国家差距的修正系数；

K_3 ——生产厂现有工艺水平与先进国家工艺水平差距的修正系数；

K_4 ——生产厂在产品的设计、生产等方面的经验与先进国家差距的修正系数；

K_5 ——生产厂的产品与先进国家结构方面差异的修正系数。

在应用中可根据实际情况对修正系数进行增补删减。

7. 可靠性框图法

可靠性框图法是以系统组成单元的可靠性预计值为基础，依据建立的可靠性框图及数学模型计算得出系统任务可靠度。其预计程序如下：

① 根据任务剖面建立系统任务可靠性框图。

② 根据相似产品法、评分分配法、应力分析法、故障率预计法等预计出单元的故障率或平均严重故障间隔时间（MTBCF）。

③ 确定单元的工作时间。

④ 根据可靠性框图计算系统任务可靠度。

8. 功能预计法

功能预计法是一种把设备或系统预期的可靠性与其功能联系起来的预计方法。该方法的适用条件是：已知设备的功能与可靠性水平的回归方程以及各个系数的数值。它以统计设备的功能特性和观测到的工作可靠性之间的相关关系为基础，最后得到重要的设备功能（从可靠性的角度而言）与可靠性的回归方程。目前，能建立这种回归方程的设备类别还很有限。

9. 上下限法

上下限法常用于复杂系统的可靠性预计，其基本思想是：由于系统的复杂性，计算其可靠度真值比较困难，于是设法预计两个近似值，一个称为可靠度上限（ R_u ），一个称为可靠度下限（ R_l ），然后取上、下限的几何平均值作为系统的可靠度预计值（ R_s ）。

上下限法实质上是一种简化了的数学模型算法。只是在预计时，将数学模型的高阶项略去，在保证精度的同时，大大简化了计算，节省了时间。在预计复杂系统可靠性，无法建立精确的数学模型时，该方法的优点较为显著。因此，这种方法一般用在比较复杂的系统上，由于上下限法需要预先知道各个单元的可靠度，因此，一般用于详细设计阶段。

上下限法的原理是根据 $R=1-F$ ，把 1 减去系统的失效概率作为可靠度预计的上限值 R_u ，而把系统的成功概率相加作为可靠度的下限值 R_l 。在计算上限的过程中，略

去了某些失效概率,这时所得出的可靠度就比实际的要高,所以定为上限。同样,在下限计算中,略去了某些成功的概率,这时所预计出来的可靠度就比实际的要低。最后把对应的可靠度上下预计值代入如下公式,即可计算出系统的可靠度。

$$R_s = 1 - \sqrt{(1 - R_u)(1 - R_l)} \quad (5-36)$$

10. 非工作状态的可靠性预计

所谓产品的非工作状态指的是电子设备和系统“可能工作而不在工作的状态”,包括运输期、储存期、冷储备备份单元的备份状态、单机工作时的关机状态,但产品发生故障的待维修状态不属预计的范围。

实践证明,长期不工作和储存的产品存在一定的功能退化。例如,空空导弹是一次性使用的武器,具有储存时间长、使用时间短、待命时间长、通电时间短、挂飞时间长、自主飞行时间短的特点。只有部分产品工作的挂飞通电时间和地面检测通电时间约占储存时间的千分之一,而全部产品工作的自主飞行时间只占挂飞通电时间的万分之一。由此可见,有些设备处于非工作状态的时间远远大于工作时间。非工作状态下电子设备可靠性水平的高低直接影响未来发挥作用的效能,直接影响电子设备的可用性。因而“产品不是用坏了,而是放坏了”的事件时有发生,这也是我们要重视电子设备和系统在非工作状态下的可靠性水平的重要性原因所在。

电子产品非工作状态可靠性预计的一般程序如下:

① 先划分可靠性预计单元,后建立系统可靠性模型。所划分的预计单元在电路功能上相对独立,非工作状态其可靠性模型一般为串联结构。

② 编制系统、设备的元器件清单。应在清单中列出元器件名称、型号规格、位号、产品标准、技术文件、封装、结构参数等。

③ 计算元器件的非工作失效率。对于采用“元器件非工作可靠性详细预计法”的按 GJB/Z 108A 第 5 章提供的非工作失效率预计模型计算其非工作失效率;对于采用“元器件非工作计数可靠性预计法”的,则由 GJB/Z 108A 第 6 章的非工作通用失效率乘以非工作质量系数,便得到某一类元器件的非工作失效率。

④ 将预计单元中各种类元器件的非工作失效率相加,由此得出预计单元的非工作失效率。

⑤ 按设备、系统的可靠性模型,逐级预计设备、系统的非工作状态可靠性。

11. 基于失效物理的预测方法

基于失效物理的预测方法,通过了解可能发生的失效及其机理,发现产品或现有技术中潜在的问题,并在问题发生前解决它们。“失效物理”方法的焦点是关注主要的失效模式,在对有关物理现象及失效机理深入认识和彻底理解的基础上,利用仿真方法或推导出定量模型进行预计。经实践证明,失效物理方法对预防、发

现、纠正与产品设计、制造和工作有关的失效是有效的，具有工程实用性。

但基于失效物理的预测方法计算量大，投入成本大，普遍适用性差，且必须同实际产品所采用的元器件、材料、工艺相结合，要量化整个系统的可靠性是困难的，其困难主要体现在系统或设备设计师对所用元器件物理结构的理解和信息了解的困难，对电路板、结构件及电装工艺的失效机理难以深入准确地掌握。

5.5.4 主要的可靠性预计标准及其发展状况

在开展可靠性预计工作时，相应的可靠性预计标准、手册是非常宝贵的借鉴工具。为了更好地了解各类产品适用的可靠性预计标准及其发展现状，本节介绍在实际开展可靠性预计工作中通常会用到的一些预计标准。

在第二次世界大战中，为了能对系统可靠性进行量化评估，美国政府采购部门着手建立一种标准化的方法来制定需求规格和预测过程。因为如果没有标准化，每个供应商的预测就只能基于他们各自的数据。这样，对于一个由不同供应商生产的元器件组成的系统，不仅将难以评估其可靠性，而且对于同样功能的元器件或不同系统设计之间的比较也造成了困难。

可靠性预计标准可以追溯到 1956 年 11 月，美国国防部可靠性分析中心 RAC 发布了以“电子设备的可靠性应力分析”为题的 TR-1100 标准。该标准介绍了元器件失效的计算值模型。此后，美国军方于 1957 年公布了 MIL-HDBK-217《电子设备可靠性预计手册》，当时预计手册中元器件失效率数据不管元器件属何类，都采用统一的环境系数。事实上不同的环境对不同元器件的影响并不完全相同。因此，美国于 1965 年对 MIL-HDBK-217 进行了重大的修改，并形成 MIL-HDBK-217A。1974 年又将 MIL-HDBK-217A 修订为 MIL-HDBK-217B。MIL-HDBK-217B 的显著特点是增补了各种元器件，特别是新型元器件的失效模式，给出了元器件失效率的数学表达式。MIL-HDBK-217B 中通常用 π 系数来表示各种应力因素对各类元器件失效率的影响。MIL-HDBK-217 的这些改进，为以后各种数据手册的编制奠定了基础。在 MIL-HDBK-217B 的基础上美国于 1979 年 4 月发布了 MIL-HDBK-217C，于 1982 年 1 月发布了 MIL-HDBK-217D。到现在为止，最新的版本是 1995 年发布的 MIL-HDBK-217F Notice II。

其后，衍生出许多与 MIL-HDBK-217 手册十分相似的可靠性预计手册，比如 Telcordia SR-332、CNET、HRD 和西门子手册，这些手册能比较快捷地估计电信类产品的可靠性，满足了电信产品可靠性预计的需求。

以下简要介绍典型的可靠性预计手册或方法，重点介绍 217PLUS 和 IEC TR 62380 的情况。

1. RDF2000

法国电信科学研究中心在对法国电信设备失效数据进行大量收集分析的基础上,于1969年制定了RDF可靠性数据分析手册,并分别于1972、1976、1982、1984、1992、1993以及2000年进行了多次改版,目前最新版次为RDF2000,是在RDF93的基础上修订更新的,采用了类似于MIL-HDBK-217系列的数学模型,但它根据法国生产的电子元器件的工艺质量、标准规范和环境应用情况对模型参数进行了调整。

2. HRD5

英国于1981年由英国系统可靠性中心及电气工程师学会汇编了《英国电子元器件可靠性数据手册》。英国手册以数据表格形式给出了100多种元器件的失效率数据。HRD5所考虑的因素,没有MIL-HDBK-217和RDF2000那样复杂,它没有列出质量系数,其基本失效率 F_b 是按照不同环境给出来的,但它却给出了MIL-HDBK-217和RDF2000所没有的储存失效率及可靠性增长系数。此外,HRD5在制订过程中对失效率是如何随时间变化的也进行了研究,从而给出手册中数据表所用的数据。同时还研究了失效率随元器件复杂度及温度而变化的规律,并调整基本数值使其最后失效率与现场数据相符。

3. Telcordia SR-332

Telcordia SR-332是从贝尔通信研究中心发展起来用于评估电信设备可靠性的预计方法,尽管贝尔预计手册是以MIL-HDBK-217为基础的,但是历经几次改版到Bellcore TR-332第6版,直至Telcordia将其发展为SR-332第1版,均较为准确地反映了电信设备的失效率水平,还给出了三种预计方法,即元器件计数法、实验室数据分析法以及基于现场数据的预计方法。

4. GJB/Z 299C《电子设备可靠性预计手册》

中国自1980年成立“中国电子产品可靠性数据交换网”以来,开始组织了电子设备和电子元器件可靠性数据的收集分析工作。在充分分析大量可靠性试验数据和现场使用数据的基础上,于1987年4月编制了中国第一部《电子设备可靠性预计手册》。1991年发布了GJB/Z 299A,1998年发布了GJB/Z 299B,2006年发布了GJB/Z 299C。

中国的电子设备可靠性预计手册,在研究了美国、法国、英国等数据手册的基础上,结合国内的具体情况,对各类元器件的预计模型、各种 π 系数、基本失效率的图表及公式进行了深入研究,给出了采用应力分析法及计数法进行电子产品可靠性预计所需要的各种信息及图表。

5. SN29500

西门子公布的可靠性预计标准以规定条件下的失效率为基础。失效率根据元器件应用与试验的经验而确定，外部来源也加以考虑。元器件分成许多组，每一组都有一个稍有不同的可靠性模型， π 因子考虑了元器件工作温度和电应力的变化。

6. 可靠性预计程序 PRISM 软件

传统的可靠性预计模型的建立包括了对经验失效率数据的统计分析。这种统计方法产生的一般是乘法模型形式，即预计失效率等于基本失效率、几个影响可靠性的应力和元器件特性变量因子之积。乘法模型形式的主要缺点是在极端的条件下（即所有因子都为最低值或最高值时）预计失效率值可变得超常的大或小。这是乘法模型的固有局限性，主要是因为明确考虑某个失效机理或某类失效机理的影响。

而美国 RAC（Reliability Analysis Center）认为加法模型更好，这种模型可以预计每个失效机理的独立失效率。每个失效率项都用适当的应力或元器件特性来加速。RAC 于 2000 年开发了一个新的方法用于评价电子系统的失效率。这一方法包括新的元器件预计模型和评价非元器件变量影响下的系统可靠性的评价方法。这一系统评价方法克服了 MIL-HDBK-217 的一些局限性。

PRISM 中给出的系统失效率模型如下：

$$\lambda_p = \lambda_{IA} (\pi_P \pi_{IM} \pi_E + \pi_D \pi_G + \pi_M \pi_{IM} \pi_E \pi_G + \pi_S \pi_G + \pi_I \pi_E + \pi_N + \pi_W \pi_E) + \lambda_{SW} \quad (5-37)$$

式中： λ_p ——系统的预计失效率；

λ_{IA} ——失效率的初步评估值；

π_P ——部件过程因数；

π_{IM} ——早期失效因数；

π_E ——环境因数；

π_D ——设计过程因数；

π_G ——可靠性增长因数；

π_M ——生产过程因数；

π_S ——系统管理过程因数；

π_I ——诱发过程因数；

π_N ——无缺陷过程因数；

π_W ——磨损过程因数；

λ_{SW} ——软件失效率预计。

失效率的初步评估值 λ_{IA} 是通过元器件可靠性预计模型结合 RAC 数据库中的失

效率数据推导出来的初步评估值（实际上为基本失效率值）。对这一失效率要用 π_i 系数来修正，该系数考虑了系统设计、生产、管理过程，以及环境、可靠性增长和早期失效等因素。

7. 217Plus

由于原 MIL-HDBK-217 可靠性预计方法存在的许多相关问题，美国已宣布在军方标准中取消 MIL-DBK-217 标准。但美国可靠性信息分析中心 RIAC（RAC 在 2005 年更名为 RIAC）在国防部的支持下于 2006 年 9 月发布了《217Plus 可靠性预计模型手册》。

217Plus 是 RIAC 开发的一种方法论和软件工具，主要用于系统可靠性方面的评估。它是 PRISM 软件工具的升级版本，并且包含的模型数是原 PRISM 的两倍。该手册发布的目的在于提供使用 217Plus 方法进行可靠性预计所需要的所有数据、信息，帮助使用者更好地理解元器件模型，由此增强 217Plus 的有效性和可信性，进而逐步取代 MIL-HDBK-217。

217Plus 同传统预计方法一样具有两个基本元素：元器件级可靠性预计和系统级可靠性预计。图 5-18 总结了 217Plus 方法对系统或产品的失效率预计流程。

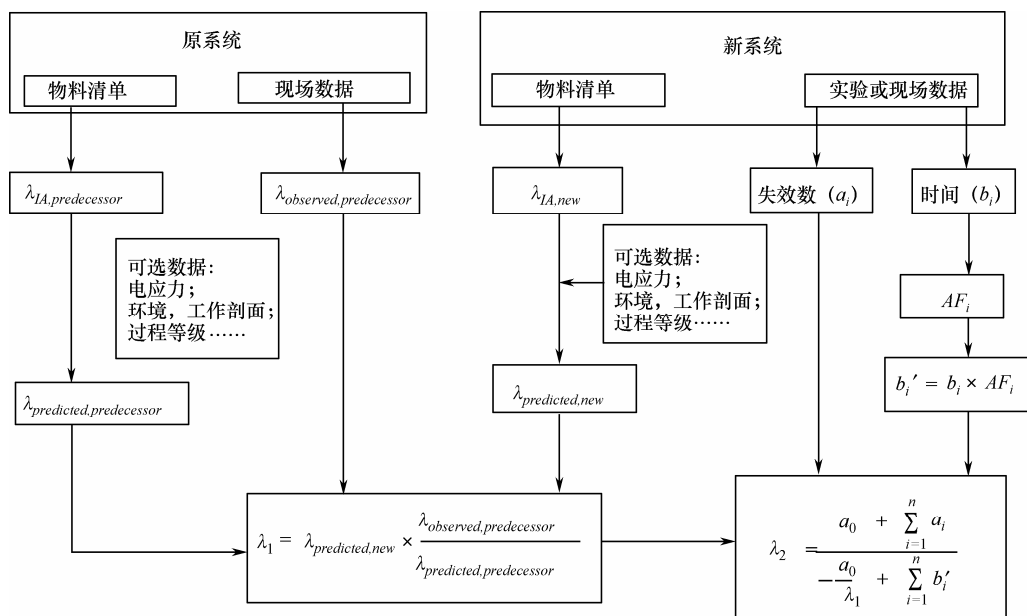


图 5-18 217Plus 失效率预计方法流程图

在这里，新系统是指与原系统基于相似技术、使用相同设计/制造工艺的系统或产品，也可以理解为原系统的优化/改进产品。 λ_{IA} 为系统初始预计失效率，是各

元器件预计失效率的累加值； $\lambda_{predicted}$ 为系统结合了过程等级等因素的预计失效率，其计算方法在系统级模型中会介绍； $\lambda_{observed}$ 为观测到的失效率，是失效率的点估计；如果新系统采用了与原系统相似的设计或生产工艺，并且使用相同的预计方法和数据，那么就可以相信新系统的预计/观测比是与原系统相似的，所以可以通过图上公式得到新系统的预计观测失效率 λ_1 ； AF_i 为第 i 组数据中，测试现场条件与实际使用条件之间的加速因子，是一个修正因子，等于测试或现场条件下预计失效率与实际使用条件下预计失效率之比； b_i' 为第 i 组数据中，试验或现场数据的有效积累时间； a_0 为与预计失效率相关的失效数的有效数字，其缺省为 0.5。 λ_2 是利用了所有可用数据信息及贝叶斯定理得到的新系统可靠性的最佳估计值，即最后得到的结果。

系统预计方法是 217Plus 和前身 PRISM 在系统可靠性预计领域的一大突破，摆脱了传统预计法的缺陷，根据实际失效原因分布，考虑了非器件因素失效率，如生产、设计的缺陷引起的失效。并且对于失效率的修正采用了过程评分、试验数据、现场数据这三种修正方法，还利用贝叶斯分析方法简化了将现场数据和试验数据整合到可靠性预计结果的过程。217Plus 方法充分利用了所有可得的数据。

8. IEC TR 62380

国际电工委员会（IEC）于 2004 年发布了可靠性预计手册 IEC TR 62380——《电子元器件、PCB 和设备可靠性预计通用模型手册》，需要注意的是 IEC TR 62380 是一份技术报告，而不是预计标准。

IEC TR 62380 中主要给出了约 19 类元器件的失效率预计模型，包括：PCB、混合集成电路、单片集成电路、二极管、晶体管、晶闸管、光电子器件、电容器、电阻器、电感器、变压器声表器件、继电器、开关、连接器、显示器、电池等。

此外，IEC TR 62380 也给出了部分器件平均寿命的计算公式，并注明器件使用时间不能超出这个平均寿命值，否则失效率不能再假定为恒量。因此 IEC TR 62380 中器件的预计失效率还是针对偶然失效期的估计，IEC TR 62380 认为早期失效率是可以忽略的，而器件的使用期限也往往达不到损耗期。对于系统可靠性，它还是认同传统预计方法：非冗余系统或设备的失效率可通过各元器件失效率的累加得到。

对于可靠性增长问题，基于 20 世纪 70—80 年代收集的现场数据分析，IEC TR 62380 认为 20 世纪 90 年代以来元器件的可靠性增长就没有再发生。只是对于集成电路，IEC TR 62380 认为：集成电路的集成密度还是在以同样的速度增长。在集成电路的预计模型中会涉及电路的生产时间，但不是因为可靠性的增长，而是基于电

路集成密度的考虑。

同 217Plus 一样，IEC TR 62380 认为要获得更精确的预计结果，必须要考虑非元器件本身引起的失效。在器件模型方面，部分模型中包含了过电应力失效率。而在系统方面，IEC TR 62380 认为由于设计、器件选择、使用等因素引起的失效是不可避免的，所以预计中不考虑这些因素。

IEC TR 62380 给出了 12 类最常见的环境类型，类似于 217F 中的环境类型。IEC TR 62380 最大的特点在于把任务剖面划分为若干相似的工作状态，主要是以热循环为依据，一般分为以下 3 个状态：设备开关状态、设备持续工作状态、设备存储或休眠状态。在每个状态下，设备周围温度都会有波动。

例如，手册中对航空电子设备任务剖面的划分：

- 状态 1：日常的开启飞行，即正常的持续工作状态。
- 状态 2：两次飞行之间的关断，此时空气调节装置还在运行。
- 状态 3：飞机着陆，非工作状态。

表 5-11 给出了典型军用、民用航空电子设备三种状态下的任务剖面。

表 5-11 IEC TR 62380 中军用、民用航空电子设备任务剖面

任务剖面阶段		设备的年工作率 (占空比)			状态 1		状态 2		状态 3	
飞机 类型	$(t_{ac})_1/^{\circ}\text{C}$	τ_1	τ_{on}	τ_{off}	n_1 循环 次数/年	$\Delta T_1/^{\circ}\text{C}$ /每次 循环	n_2 循 环次数 /年	$\Delta T_2/^{\circ}\text{C}$ / 每次循环	n_3 循环 次数/年	$\Delta T_3/^{\circ}\text{C}$ / 每次循 环
A340	40	0.61	0.61	0.39	330	$\frac{\Delta T_j}{3} + 30$	330	$\frac{\Delta T_j}{3} + 15$	35	10
A330	40	0.54	0.54	0.46	330	$\frac{\Delta T_j}{3} + 30$	660	$\frac{\Delta T_j}{3} + 15$	35	10
商务 飞机	40	0.22	0.22	0.78	330	$\frac{\Delta T_j}{3} + 30$	300	$\frac{\Delta T_j}{3} + 30$	65	10
战斗 机	60	0.05	0.05	0.95	200	$\frac{\Delta T_j}{3} + 50$	0	0	165	10
巡逻 机	50	0.09	0.09	0.91	300	$\frac{\Delta T_j}{3} + 40$	0	0	65	10
直升 机	50	0.06	0.06	0.94	300	$\frac{\Delta T_j}{3} + 40$	0	0	65	10

对于更为复杂的任务剖面，器件所有的工作或非工作状态的温循都要考虑。

5.5.5 进行可靠性预计时的注意事项

① 可靠性预计作为一种工具主要用于选择最佳方案，在选择了一设计方案后，通过可靠性预计可以发现设计中的薄弱环节，以便采取改正措施。另外，通过可靠性预计和分配的相互配合，可以把规定的可靠性指标合理分配给产品的各组成部分。但需要注意，虽然通过可靠性预计可以推测产品能否达到可靠性要求，但绝不能把预计值作为可靠性要求满足程序的依据。产品可靠性最终结果只能依靠可靠性试验确定。

② 产品的复杂程度、研制费用及进度要求等直接影响着可靠性预计的详略程度，产品不同及所处研制阶段不同，可靠性预计的详细程度及方法也不同。可靠性预计可在不同的层次上进行。约定层次的确定必须考虑产品的研制费用、进度要求和可靠性要求，应与进行 FMECA 的最低产品层次一致。

不同研制阶段预计方法的选取可参考表 5-12。

表 5-12 不同阶段的可靠性预计方法选用参考表

研制阶段	可靠性预计方法
方案论证	功能预计法、相似产品法、可靠性框图法
初步设计	评分法、元器件计数法、相似产品类比论证法，可靠性框图法
详细设计	故障率预计法、应力分析法、上下限法、可靠性框图法

- 方案论证阶段。在这个阶段，信息的详细程度只限于系统的总体情况、功能要求和结构设想，一般采用功能预计法或相似产品法，以工程经验来预计系统的可靠性，为方案决策提供依据，称此阶段为“可行性预计”阶段。
- 初步设计阶段。该阶段已有了工程图或草图，系统的组成已确定，可采用元器件计数法、专家评分法、相似产品类比论证法预计系统的可靠性，发现设计中的薄弱环节并加以改进，称此阶段为“初步预计阶段”。
- 详细设计阶段。这个阶段的特点是系统的各个组成单元都具有了工作环境和应力使用应力的信息，可采用应力分析法或故障率预计法来较准确地预计系统的可靠性，为进一步改进设计提供依据，也称此阶段为“详细预计阶段”。

③ 应尽早利用可靠性预计结果，为转阶段决策提供信息，为此，可靠性预计的时机应在合同及有关文件中予以规定。

④ 基本可靠性预计应全面考虑从产品接收到退役期间的可靠性，即应是全寿命周期的可靠性预计。产品在整个寿命周期内除工作状态外，还处于不工作（如待

命、待机等)、储存等非工作状态。应分别计算各状态下的故障率,然后加以综合,预计出装备可靠性值。任务可靠性预计应考虑每一任务剖面的可靠性要求。

⑤ 通过预计,若基本可靠性不足,可通过简化设计、采取高质量等级的元器件和零部件、改善应力条件、调整性能容差等措施来弥补。但采用冗余技术会增加产品的复杂程度、降低基本可靠性。必要时,应重新进行可靠性分配。

⑥ 可靠性预计值必须大于规定值。预计结果不仅用于指导设计,还可为可靠性试验、制订维修计划、保障性分析、安全性分析等提供信息。

⑦ 订购方应在合同说明中明确:产品的寿命剖面 and 任务剖面;确认的预计方法;失效率数据的来源;由订购方指定的产品,应提供其可靠性水平,以及相关的使用与环境信息;需提交的资源项目等内容,以保证可靠性预计的合理性和准确性。

5.6 可靠性仿真

众所周知,可靠性是设计特性,在设计与制造阶段形成。从研制早期抓好可靠性工作,是提高产品可靠性的有效途径。可靠性作为一门系统工程科学,经过半个多世纪的发展已经形成了较为完整、健全的体系。传统的可靠性设计、分析与试验方法在许多领域取得了丰硕的成果,而可靠性仿真作为一门新兴的可靠性技术正在兴起,它必将为可靠性设计分析工作提供一种更强有力的工具。

5.6.1 可靠性仿真的内涵、条件和优势

所谓仿真(Simulation),就是用模型代替实际系统进行试验。按模型的不同,仿真可分为数学仿真、物理仿真、半实物仿真三种。三种方法根据不同的需要应用在不同场合或阶段。

仿真最初被应用于实际系统进行试验有危险和花费很大的领域,如航空、航天、武器系统等;后来逐渐运用到虽然可在实际系统上进行试验,但花费较大、耗时较长、不大方便的一些领域,如冶金、化工、电力等。近十年来,则进一步扩大到制造、交通、环境、生态、生物、社会、经济等领域。随着仿真技术、计算机技术、建模水平的快速发展,仿真在国民经济的众多领域,取得了较好的社会效益和经济效益。

仿真主要用于研究系统方案的可行性、调整系统结构参数、提高系统精度、预测某项目前景等方面。它与实际系统研究法、解析分析法相比,各有特点,如表 5-13 所示。

表 5-13 仿真方法、实际系统法、解析法对比表

性能\方法	仿真技术	实际系统研究法	解析分析法
可能性	只要能建立系统模型，就能进行	系统尚未建立，则不可能；有的自然系统实验周期太长，也不可能	有的系统无法建立解析模型，因此，不可能利用解析方法
安全性	无危险	有危险（人身、设备）	无危险
经济性	花费不多	费用很大	花费不多
耗时性	中等	长	短
准确性	可以做到很准确	十分准确	要做很多假设，因此误差较大
方便性	可以做到十分方便	受现场限制，很不方便	方便

进行可靠性仿真需要满足一定的条件：一是组成系统中的各个单元及其相应的随机变量的理论分布已经确定；二是能够对相应的理论分布产生各种随机变量；三是判定系统成功或失效的各种具体规则已经确立。

由此可见，进行可靠性仿真，主要是确定系统中各个组成单元相应的各种随机变量的理论分布，以及建立判定系统成功或失效的各种具体规则。这些规则，实际上就是系统与组成系统的各个单元成功、失效的相互关系，也就是系统的可靠性模型。因此，对于简单的可靠性模型，可以通过单元的理论分布直接求系统的理论分布，从而求得系统的可靠性，无须通过可靠性仿真过程。

对于能够产生相应理论分布的随机数，按照判定规则确定成功或失效，这完全可以由计算机承担。

随着仿真技术的不断发展，仿真技术应用到了可靠性研究上，形成了可靠性仿真。针对可靠性研究的特点，可靠性仿真一般采用数学仿真方法。所谓数学仿真就是用数学模型代替实际系统在计算机上进行试验。与其他方法相比，数学仿真具有以下优点：

- 精度高。仿真计算机是数学仿真的主要硬件设备，随着仿真机技术的发展，计算机运算精度有了很大的提高，这保证了试验结果的精确性。同时，数学仿真试验结果的逼真度和置信度，主要依赖于建立的数学模型的准确性。现有的可靠性和仿真技术已经能较好地解决可靠性建模这一问题。
- 对计算机要求较低。可靠性仿真不要求实时仿真，因此在一般的个人微机、工作站上就可以进行，而不需专门的、昂贵的仿真机（小型机、巨型机等）。这一点更有利于可靠性仿真工作的开展。
- 难度较低。可靠性数学模型变为计算机上运行的仿真模型，可以直接利用系统数学模型中各种坐标系及其变换关系进行，不必考虑因实物接入而带来的各坐标系之间的协调转换，降低了实现仿真的难度。
- 成本低。数学仿真突出的优点之一，就是所有试验封闭在计算机上进行，它不需要实物的参与，又可以进行大量的、重复性的试验，节省了可靠性工程

经费的投入。可靠性仿真特别适用于可靠性统计试验。

5.6.2 可靠性仿真的一般流程

对于庞大、复杂的系统，其各分系统、组合、元器件、零件都有不同的失效类型和故障模式，传统的分析方法研究十分困难。可靠性仿真则可以较好地解决这个问题。它既可以应用于可靠性设计、分析中，也可以应用于可靠性试验中；既可以应用于可靠性统计试验，又可以应用于可靠性工程试验；既可以先对各分系统，如电气、液压等重点分系统进行可靠性仿真，进而依据这些结果对全系统进行可靠性仿真，也可以直接对全系统进行可靠性仿真，具有广泛的应用范围。

可靠性仿真在不同的研制阶段也具有不同的做法。在方案论证阶段，利用可靠性设计手册提供的可靠性预计数据、可靠性分配数据、相似产品或经验数据进行仿真试验，针对系统给出比较粗略的估计；在工程研制阶段，就可以利用有关的试验数据进行仿真试验，通过修改实际系统，可以提高系统可靠性水平，通过对仿真结果的统计分析，可以实现对系统可靠性精确的评估；在产品使用阶段，通过对发生故障的复现、排除，实现对产品的改进设计。

可靠性仿真的步骤一般包括：

- ① 定义系统，确定可靠性仿真的目的和范围。
- ② 收集数据，建立可靠性数据库。广泛收集可靠性数据，对数据进行加工、处理，得出各分系统，以及各分系统内各元器件、组合、部件等的寿命分布类型和可靠性参数值，从而建立系统的可靠性数据库。
- ③ 建立可靠性模型（数学模型）。利用系统的热设计、冗余设计、降额设计，以及积累零件、元器件、部件、组合和分系统的失效模式等数据，采用可靠性框图、FTA等手段，建立可靠性模型。
- ④ 建立可靠性仿真模型。根据可靠性模型的形式、计算机类型以及试验要求将可靠性模型转变成适合计算机处理的形式，即可靠性仿真模型，并依据有关参数进行仿真模型的验证，确定模型的有效性。
- ⑤ 编制仿真程序。利用仿真软件将可靠性仿真模型输入计算机，并对仿真程序要使用的数组定维、设置工作单元位置、输入可靠性仿真参数、初始条件、规定输出打印间隔、打印数据和绘图比例尺等。
- ⑥ 可靠性仿真试验。依据仿真目的，在可靠性仿真模型上进行大量的仿真试验。仿真不同于一般的科学计算，它要求体现出“在模型上进行试验”这个含义，也就是在仿真试验时，工程技术人员就像在真实系统上进行试验那样可以观察系统的动态过程，适时地改变系统的初始条件和有关参数，甚至结构模型，实现人机交互功能。



⑦ 可靠性仿真结果的分析与评定。对于复杂的随机过程，一般采用蒙特卡洛法 (Monte Carlo) 等统计方法，通过选择不同的随机初始条件和随机输入函数，对可靠性仿真系统进行大量的统计计算，并得出系统变量的统计特性。

5.6.3 可靠性仿真的技术难点

在可靠性仿真中有两个比较重要的环节：一是数学模型是否反映真实系统，即数学模型的验证；二是校正仿真模型是否正确实现了数学模型，即仿真模型的校验，只有当数学模型和仿真模型都得到了验证，可靠性仿真才是可信的。

建立可靠性仿真模型需要可靠性工程专业技术人员和仿真专业技术人员的密切配合。在可靠性分析模型基础上，将分析程序与相应的可靠性仿真程序相连接，并将可靠性分析模型中的一些参数用随机变量描述。对于模型中的参数，有的可以直接从有关手册中查得，有的则要通过试验求得。对于随机变量的分布参数，有的可以直接根据工程判断，认可后使用，有的应安排一些试验验证后使用，还有的须经有关数据变换后才能使用。工程研制部门应及时提供可靠性仿真必需的有关试验参数，以切实保证可靠性仿真模型的需要。

为确保可靠性仿真结构与实际产品试验结果接近，在建立可靠性仿真模型之后，要进行如下工作：

- 模型校验，主要验证仿真模型与理论模型是否相符合。
- 程序校验，在计算机上运行可靠性仿真程序，通过试算等手段对程序进行测试。
- 模型验证，将仿真试验结果与真实试验结果相对比，对可靠性仿真模型进行部分修改，逐步完善模型。
- 模型确认，用经过验证后的仿真模型进行仿真试验，并将仿真试验结果与有关的试验数据进行对比分析，在此基础上可邀请各方面专家对仿真模型予以确认。经过确认的模型认为是可信的模型，在此模型上进行大量的仿真试验，同时给出可靠性仿真结果。

正确建立可靠性仿真模型和可靠性仿真模型的验证确认，是可靠性仿真成败的关键，也是顺利完成仿真试验，得出令人信服的结果的保证。

5.7 故障模式、影响及危害性分析 (FMECA)

5.7.1 FMECA 的方法概述

FMECA 是一种系统化的可靠性分析程序。它通过系统的分析，确定元器件、

零部件、设备、软件在设计 and 制造过程中所有潜在的故障模式，以及每一故障模式的原因和影响，并按故障影响的后果对每一潜在故障模式划等分类（危害度分析），以便找出潜在的薄弱环节，并提出改进措施。

从当前国内外应用 FMECA 技术的情况看，FMECA 方法可概括为两大类，即单因素 FMECA 方法和综合因素 FMECA 方法。其中单因素 FMECA 方法又可分为设计 FMECA（包含功能 FMECA、硬件 FMECA、软件 FMECA、损坏模式及影响分析 DMEA）、过程 FMECA；综合因素 FMECA 方法主要考虑与其他可靠性等分析方法相结合，包括 FTA（Fault Tree Analysis，故障树分析）和 ETA（Event Tree Analysis，事件树分析）等，如图 5-19 所示。

在产品寿命周期的各阶段，根据具体的要求选用不同的 FMECA 方法。选择 FMECA 的方法如表 5-14 所示。

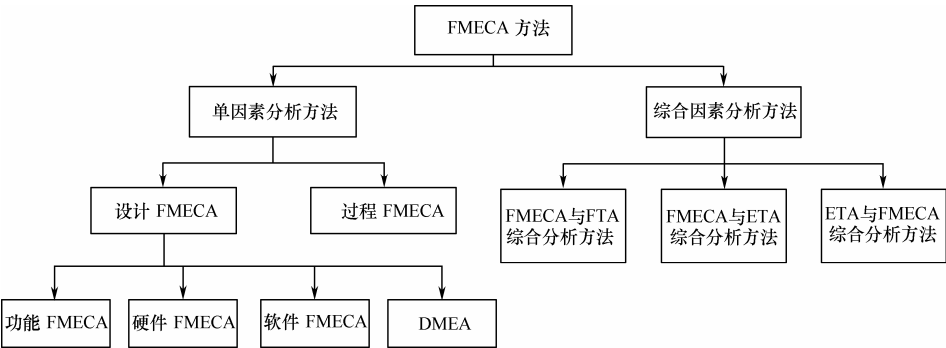


图 5-19 FMECA 方法

表 5-14 不同阶段 FMECA 方法的选取

阶 段	方 法	目 的
论证、方案阶段	功能 FMECA	分析研究产品功能设计的缺陷与薄弱环节，为产品功能设计的改进和方案的权衡提供依据
工程研制与定型阶段	功能 FMECA 硬件 FMECA 软件 FMECA 损坏模式及影响分析（DMEA） 过程 FMECA	分析研究产品硬件、软件、生产工艺、生存性与易损性设计的缺陷及薄弱环节，为产品的硬件、软件、生产工艺、生存性与易损性设计的改进提供依据
生产阶段	过程 FMECA	分析研究产品生产工艺的缺陷和薄弱环节，为产品生产工艺的改进提供依据
使用阶段	硬件 FMECA 软件 FMECA 损坏模式与影响分析（DMEA） 过程 FMECA	分析研究产品使用过程中可能实际发生的故障、原因及其影响，为提高产品使用可靠性，进行产品的改进、改型或新产品的研制，以及使用维修决策等提供依据

FMECA 是分析产品所有可能的故障模式及其可能产生的影响,并按每个故障模式产生影响的严重程度及其发生概率予以分类的一种归纳分析方法,是属于单因素的分析方法。

FMECA 由故障模式及影响分析(FMEA)、危害性分析(CA)两部分组成。只有在进行 FMEA 的基础上,才能进行 CA。

FMECA 是产品可靠性分析的一个重要的工作项目,也是开展维修性分析、安全性分析、测试性分析和保障性分析的基础。

在产品寿命周期的各阶段,采用 FMECA 的方法及目的略有不同。虽然各个阶段 FMECA 的形式不同,但根本目的均是从不同角度发现产品的各种缺陷与薄弱环节,并采取有效的改进和补偿措施以提高其可靠性水平。

产品的设计 FMECA 工作应与产品的设计同步进行。产品在论证与方案阶段、工程研制阶段的早期主要考虑产品的功能组成,对其进行功能 FMECA;当产品在工程研制阶段、定型阶段,主要是采用硬件(含 DMEA)、软件的 FMECA。随着产品设计状态的变化,应不断更新 FMECA,以及时发现设计中的薄弱环节并加以改进。

过程 FMECA 是产品生产工艺中运用 FMECA 方法的分析工作,它应与工艺设计同步进行,以及时发现工艺实施过程中可能存在的薄弱环节并加以改进。

在产品使用阶段,利用使用中的故障信息进行 FMECA,以及时发现使用中的薄弱环节并加以纠正。

5.7.2 FMECA 的作用

FMECA 分析技术作为一项可靠性工程的基础工作,在可靠性分析、维修性分析、保障性分析、测试性分析、安全性分析中都起到重要作用。

1. FMECA 在可靠性分析中的应用

FMECA 是 GJB 450A《装备可靠性工作通用要求》中要求开展的一项可靠性设计与分析工作,通过 FMECA 可确定可靠性关键产品。GJB 450A 中指出:可靠性关键产品是指该产品一旦发生故障就会严重影响系统的安全性、可用性、任务成功、维修及寿命周期费用。可靠性关键产品是进行可靠性设计分析、可靠性增长试验、可靠性鉴定试验的主要对象,必须认真做好可靠性关键产品的确定和控制工作。危害性分析(CA)的目的就是对产品每个故障模式的严重程度及其发生概率所产生的综合影响进行分类,以全面评价产品中所有可能出现的故障模式影响。显然,FMECA 工作输出的结果之一就是产品的“可靠性关键产品清单”。

在具体应用 FMECA 来确定可靠性关键产品清单时,可在危害性矩阵图上划定响应的范围,作为确定可靠性关键件的依据。通常情况下,可以取严酷度为 I、II

类的故障模式产品作为可靠性关键产品。

2. FMECA 在维修性分析中的应用

FMECA 是直接从产品出发考虑其故障模式、影响及其危害性的严重程度；而维修性分析则主要是从产品维修的角度出发，考虑产品具备好修、易修的特性。维修性分析工作不应单纯地只从产品设计方案入手，应动态地考虑整个维修过程中维修人员与被修对象之间的相互关系，具体包括：相对位置、交互类型（如拉、推、抬等操作类型）、相对活动空间等。因此，FMECA 与维修性分析工作有如下关系：

- 利用 FMECA 结果，针对故障的基本维修措施进一步确定维修性的设计与分析要求。
- 利用 FMECA 技术，研究维修中由于人机交互而引发“新”的故障模式，并进行相应的 FMECA，从而为维修性设计分析中的维修安全、防差错措施等方面提供信息。

FMECA 给出的故障模式及其相应的维修措施正是开展维修性分析的输入条件；FMECA 中给出的故障模式严酷度可作为开展维修性权衡分析时的依据之一；FMECA 中给出的设计改进和使用补偿措施可作为维修性设计分析的参考内容。

根据 FMECA 的结果，尤其是“设计改进、使用补偿措施”的内容，为维修性设计要求提供了重要的参考信息。在进行了 FMECA 之后，其中排除故障所需要的“基本维修措施”信息可用于确定维修性定性、定量要求，也可直接用于开展维修过程的 FMECA 工作。这样，在定义人机系统的基础上分析获得新的故障模式，并开展相应的 FMECA 工作，其结果与产品设计 FMECA 的结果统一处理，一并在维修性的设计分析工作中进行考虑，从而得到更为具体的维修性设计要求。

3. FMECA 在安全性分析中的应用

FMECA 可以用于系统安全性分析，特别适用于因硬件事故的风险分析。用 FMECA 方法进行安全性分析可以系统地识别所有可能的故障模式，发现潜在的故障危险源；确定每个故障模式可能产生的安全性影响，并有助于确定危险的严重性和可能性，通常是根据每个故障模式的故障影响、严酷度、发生概率或频率来度量风险。可帮助设计人员识别、去除或控制有危险性的故障模式和安全性关键产品，降低其对系统及相关使用者的危害程度；可及时发现安全性的薄弱环节，进而制定有效的改进措施，以提高产品安全性水平。

FMECA 在安全性分析中的应用是对 FMECA 应用的扩充。既可在进行可靠性 FMECA 分析时同步考虑每个故障模式的危险性，也可以在完成可靠性 FMECA 之后针对每个故障模式进行专门的安全性分析和风险评价。例如，根据直升机的 FMECA 分析确定的 I、II 类的故障模式，结合故障树技术进行直升机 I、II 类故障

模式所导致的 I、II 类事故（例如双发停车）的发生概率计算，根据计算结果判断系统的事故发生概率是否在可接受范围或者是否满足适航性要求。

需要注意的是，用于安全性分析时，FMECA 可在各个分析约定层次展开，但一般应用在关键的系统和设备上，以减少工作量。

FMECA 在安全性分析中的应用步骤如图 5-20 所示。

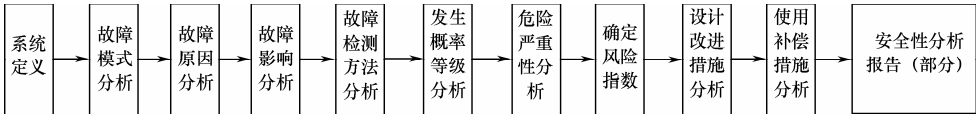


图 5-20 FMECA 在安全性分析中的应用流程图

4. FMECA 在测试性分析中的应用

FMECA 是测试性分析的重要基础之一。FMECA 的结果，尤其是获得的故障模式等内容，为产品的测试性指标分配、测试性预计、故障注入或模拟、优选测试点以及具体操作等方面提供支持。

在 FMECA 中获得的故障模式、影响和故障率数据等信息的基础上，进行测试性指标的分配、指导测试点的选取、固有测试性和机内测试（BIT）的设计；收集包括故障检测能力和故障隔离能力等内容的测试性相关资料；根据收集到的资料进行测试性指标预计，并判断是否符合规定的测试性要求；当预计值不符合要求时，要对系统的测试性设计进行改进，再针对改进的产品进行测试性资料收集及指标预计，如此反复迭代，直至符合要求；当预计值符合要求时，将 FMECA 和测试性相关分析的结果写成分析报告。

FMECA 在测试性分析中的应用步骤如图 5-21 所示。

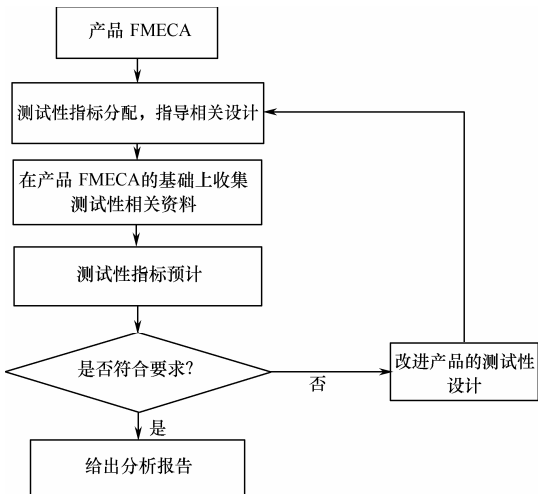


图 5-21 FMECA 在测试性分析中的应用流程图

5. FMECA 在保障性分析中的应用

在装备的技术保障中包含两部分内容,即使用保障与维修保障。引起维修的原因是装备的故障,当故障发生后,考虑装备如何设计可便于修理是维修性的工作范畴。但是,维修不是没有条件的,完成再简单的维修工作也需要保障资源的支持,例如维修人员、维修工具等。装备保障性工作,是从装备自身的设计特性与规划的保障资源能够满足战备完好性要求两个角度出发,因此其工作的内涵要比维修性、测试性更为宽广。FMECA 是保障性分析的重要基础之一,其在保障性分析中的作用可简单概括为:

- 是确定重要预防性维修工作项目和要求的依据之一。
- 是确定修复性维修工作项目和要求的依据之一。
- 为确定维修保障资源提供故障模式及有关信息。

FMECA 在保障性分析中的应用步骤如图 5-22 所示。

具体而言,对于重要功能产品,一是需要根据其故障模式开展以可靠性为中心的维修分析(RCMA)工作,并从分析结果确定产品所需要开展的预防性维修工作项目及维修间隔期;二是需要从 FMECA 给出的故障信息直接确定产品需要开展的修复性维修工作;三是对上述两种维修(预防性维修、修复性维修)工作经“使用与维修工作分析”(O&MTA)后,可以确定所需的维修保障资源需求,包括资源的种类、数量、功能设置性能要求等。在某些情况下,FMECA 给出的修复性维修任务可直接输入到修理级别分析(LORA)中,以确定执行该任务的场所。

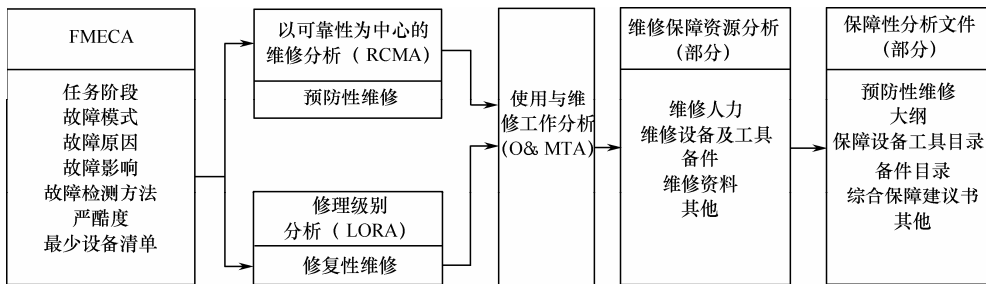


图 5-22 FMECA 在保障性分析中的应用流程图

5.7.3 FMECA 的实施要求和注意事项

FMECA 方法,需要相应的管理制度,以及人力、物力保证才能有效果,因此,在实施 FMECA 技术时,需要注意如下几点。



① FMECA 应在规定的产品层次上进行。开展 FMECA 分析工作,目的是通过分析发现潜在的薄弱环节(即可能出现的故障模式),分析每种故障模式可能产生的影响(对寿命剖面和任务剖面的各个阶段可能是不同的),以及每种影响对安全性、战备完好性、任务成功性、维修及保障资源要求等方面带来的危害。对每种故障模式,通常用故障影响的严重程度以及发生的概率来估计其危害程度,并根据危害程度确定采取纠正措施的优先顺序,整个分析过程的工作量较大。另外,近年来,一些企业在一些重要产品,考虑从元器件级开始开展 FMECA 工作。但是,在开展元器件级 FMECA 工作时,考虑到元器件的数量一般较多,如果每个器件都开展 FMECA 工作,是不现实的做法,因此,在开展 FMECA 工作时,需要定义好开展 FMECA 的产品层次,以及开展 FMECA 的细化程度、深度。

② FMECA 应与产品设计工作同步并尽早开展,当设计、生产制造、工艺规程等进行更改,对更改部分应重新进行 FMECA。

③ FMECA 的对象包括电子、电气、机电、机械、液压、气动、光学结构等硬件和软件,并应深入到任务关键产品的元器件或零件级。应重视各种接口(硬件之间、软件之间及硬件软件之间)的 FMECA,进行硬件与软件相互作用分析,以识别软件对硬件故障的响应。

④ 应进行从设计到制造的 FMECA,针对工艺文件、图样(如电路板布局、线缆布线、连接器锁定)、硬件制造工艺等进行分析,以确定产品从设计到制造过程中是否引入了新的故障模式,应以设计图样的 FMECA 为基础,结合现有工艺图样和规程进行分析。

⑤ 应按下列任一原则,确定进行 FMECA 的最低产品层次:

- 与实施保障性分析的产品层次一致,以保证为保障性分析提供完整输入。
- 可能引起灾难和致命性故障的产品。
- 可能发生一般性故障但需要立即维修的产品。

⑥ FMECA 应为转阶段决策提供信息,在有关文件(如合同、FMECA 计划)中应规定进行 FMECA 的时机和数据要求。

⑦ 开展 FMECA 工作时,关键是故障模式数据的积累。在积累产品的故障模式数据时,可考虑开展以下几个方面的工作:

- 记录、收集产品研制过程中的设计、试验出现的故障信息。
- 收集产品在生产、使用中的故障信息。
- 借鉴 FMD 2013、GJB/Z 299C 等标准手册,梳理可借鉴的故障模式信息。
- 建立故障模式收集、分析信息系统,将所有产品的故障信息进行集中管理。

5.7.4 FMECA 的工作内容和一般步骤

FMECA 是一个反复迭代、逐步完善的过程。FMECA 的主要工作内容和实施步骤如下:

- ① 准备工作——收集被分析对象(产品)的有关信息;策划 FMECA 工作的总要求。
- ② 系统定义——对被分析对象进行功能分析、绘制框图。
- ③ 确定产品所有可能的故障模式——按故障判据、相似产品、试验信息、使用信息和工程经验等方面确定产品所有可能的故障模式。
- ④ 确定每个故障模式可能的原因及其故障发生概率等级——按产品内部、外部和工程经验等相关情况确定产品故障模式的原因及其发生概率等级。
- ⑤ 确定每个故障模式可能的影响——按每个故障模式分别对自身、高一层次和最终影响进行分析,并确定其严酷度类别。
- ⑥ 确定每个故障模式可能的检查方法——按每个故障模式的原因、影响确定其检查方法。
- ⑦ 制订每个故障模式的设计改进、使用补偿措施。
- ⑧ 按每个故障模式可能发生的概率等级与严酷度等级,或危害度/风险优先数进行排序——根据每个故障模式发生概率与严酷度等级,或危害度/风险优先数的大小进行其优先排序。
- ⑨ 确定薄弱环节及关键项目——按每个故障模式的排序结果识别薄弱环节和关键项目,并列出严酷度为 I、II 类的单点故障模式清单、关键项目清单、不可检测故障模式项目清单等。
- ⑩ 判断是否需要设计改进——若要设计改进,则反馈从系统定义处重新进行分析,反之结束分析。
- ⑪ 提供 FMECA 报告——根据设计认可后,提供 FMECA 报告。

FMECA 工作的一般流程如图 5-23 所示。

要做好 FMECA 工作,首要问题是制订 FMECA 计划。FMECA 计划包括为实现可靠性要求,并随着设计的更改适时地进行 FMECA,以及利用分析结果为可靠性设计提供支持。

在 FMECA 计划中应规定产品寿命周期的不同阶段所选用的 FMECA 方法、表格格式、定义约定层次、编码体系、任务描述、故障判据、严酷度类别、所需的主要信息(输入要求)、FMECA 报告(输出结果)、评审、职责与分工等主要内容,并包括完成 FMECA 工作的步骤、实施和工作进度要求等。FMECA 计划应与产品可靠性、维修性、安全性、测试性、保障性等工作要求,以及有关标准要求相互协

调、统筹安排等，具体说明如下。

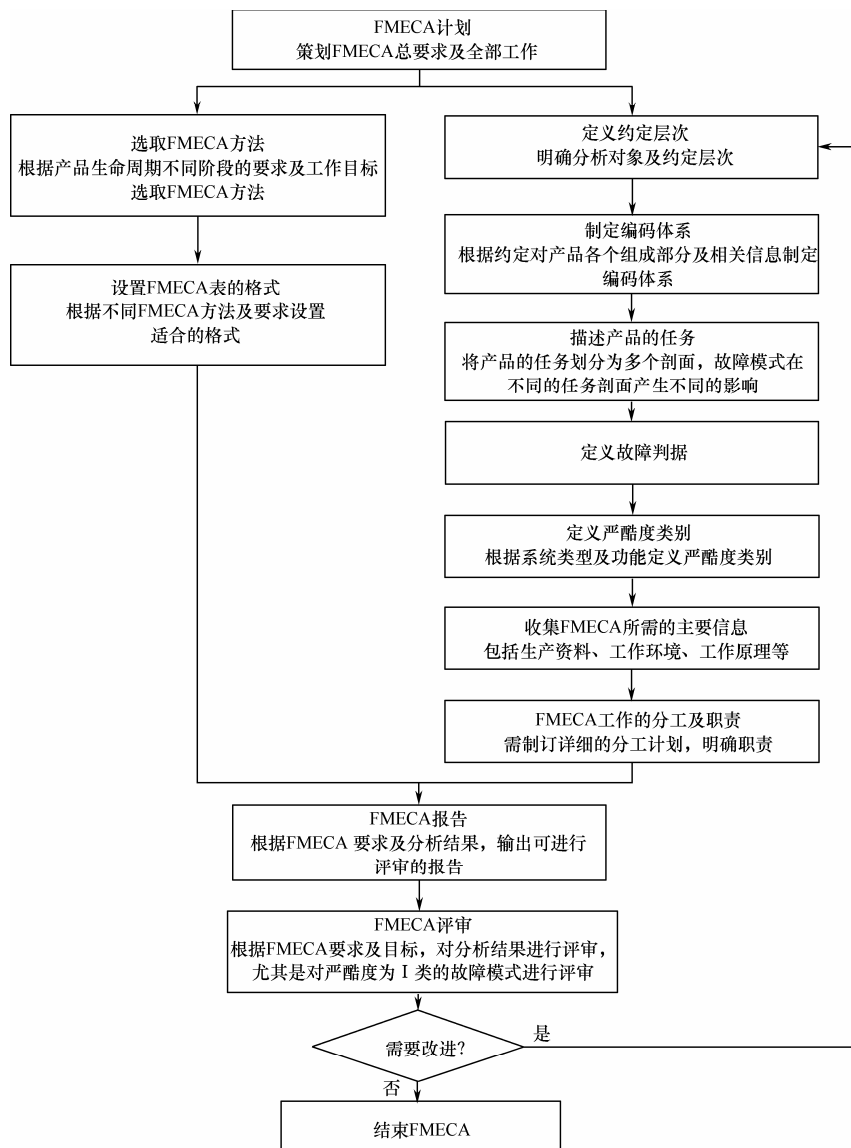


图 5-23 FMECA 工作的一般流程

1. FMECA 方法的选取

根据产品寿命周期不同阶段的需求，按照表 5-14 的内容选用不同的 FMECA 方法，并针对被分析对象的技术状态、信息量等情况，选取一种或多种 FMECA 方法进行分析。

2. FMECA 表的格式

根据表 5-14 的内容选用不同的 FMECA 方法, FMECA 表可按被分析对象的实际情况进行综合、选取、增删, 例如 FMEA 表和 CA 表可合并为 FMECA 表。

3. 定义约定层次

在对产品实施设计 FMECA 时, 应明确分析对象, 即明确约定层次的定义; 对过程 FMECA 时, 可将产品工艺流程中的各个环节作为分析对象, 考虑工艺中可能发生的缺陷对下一道工序、被加工产品或最终产品的影响。

约定层次既可以按产品的功能层次关系定义, 又可按产品的硬件结构层次关系定义。具体选用何种约定层次划分方法, 将取决于分析中所选用的 FMECA 方法。当选用功能 FMECA 方法时, 应针对产品的功能层次关系划分约定层次; 当选用硬件 FMECA 方法时, 应针对产品的硬件结构层次关系划分约定层次。

在 FMECA 中的约定层次, 划分为“初始约定层次”、“约定层次”和“最低约定层次”。例如某型系统约定层次的划分示例见图 5-24。

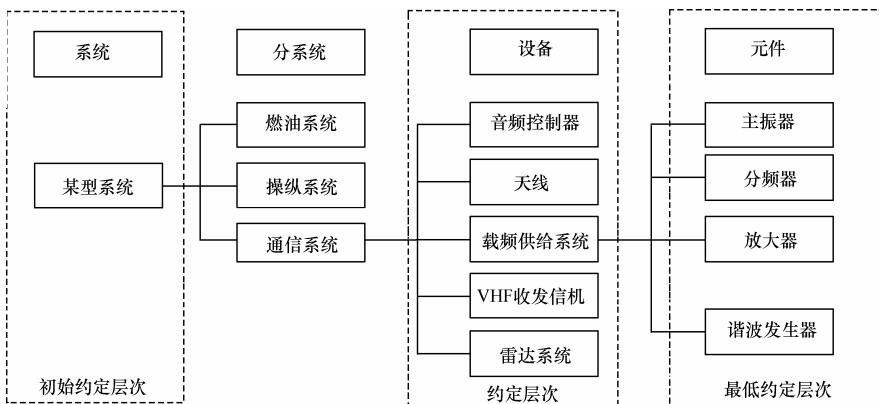


图 5-24 某型系统约定层次划分

4. 制定编码体系

为了对产品的每个故障模式进行统计、分析、跟踪和反馈, 应根据产品的功能、结构分解或所划分的约定层次, 制定编码体系。其注意事项是: 编码体系应符合产品功能及结构层次的上、下级关系; 能体现约定层次的上、下级关系, 与产品的功能框图和可靠性框图相一致; 符合或采用有关标准或文件的要求; 对产品各组成部分应具有唯一、简明和适用等特性; 与产品的规模相一致, 并具有一定的可追溯性。

5. 描述产品的任务

在 FMECA 工作中应对产品完成任务的要求及其环境条件进行描述, 这种描述一般用任务剖面来表示。任务剖面是指产品在完成规定任务时间内所经历的事件和

环境, 时序的描述, 示例见图 5-25。

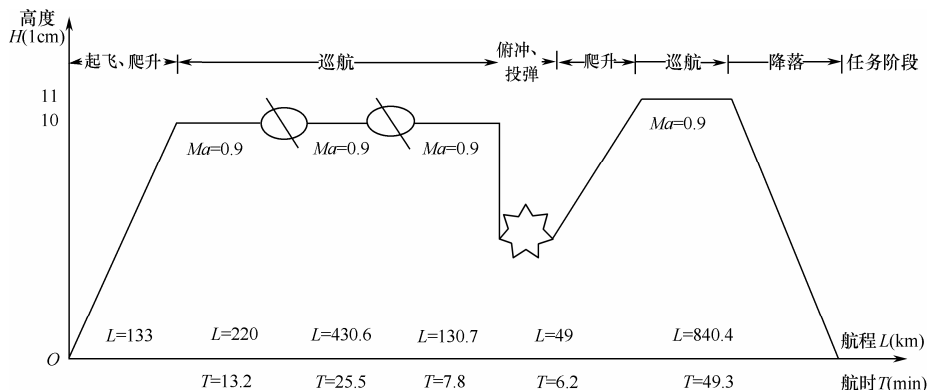


图 5-25 某型战斗机的飞行任务剖面

若被分析的产品存在多个任务剖面, 则应对每个任务剖面分别进行描述; 若被分析的产品的每一个任务剖面又由多个任务阶段组成, 且每一个任务阶段, 又可能有不同的工作方式, 则对此情况均需进行说明或描述。

6. 定义故障判据

(1) 定义故障判据的依据

故障判据的依据如下:

- 产品在规定的条件下和规定时间内, 不能完成规定的功能。
- 产品在规定的条件下和规定时间内, 某些性能指标不能保持在规定的范围内。
- 产品在规定的条件下和规定时间内, 引起对人员、环境、能源和物资等方面的影响超出了允许范围。
- 技术协议或其他文件规定的故障判据。

(2) 定义故障判据的原则

故障判据是判别产品故障的界限。它一般是由承制方和订购方共同根据产品的功能、性能指标、使用环境等允许极限进行确定的。

(3) 定义故障判据的注意事项

应对产品的组成、功能、技术要求和进行 FMECA 工作的目的等有清晰地理解, 进而针对特定产品准确地给出故障判据的具体内容 (包含功能界限和性能界限等), 以避免 FMECA 工作的随意性和模糊性。

7. 定义严酷度类别

在进行故障影响分析之前, 应对故障模式的严酷度类别 (或等级) 进行定义。

它是根据故障模式最终可能出现的人员伤亡、任务失败、产品损坏（或经济损失）和环境损害等方面的影响程度进行确定的。

定义严酷度类别时，需要注意以下几个事项：

- 严酷度类别仅是按故障模式造成的最坏的潜在后果进行确定的。
- 严酷度类别仅是按故障模式对“初始约定层次”的影响程度进行确定的。
- 严酷度类别划分有多种方法，但对同一产品进行 FMECA 时，其定义应保持一致。

8. FMECA 所需的主要信息

FMECA 所需的主要信息来源见表 5-15。

表 5-15 FMECA 所需的主要信息来源

序号	信息来源	从信息来源中可获取 FMECA 所属的主要信息	所获信息的作用
1	技术规范与研制方案	从设计技术规范和研制方案中获取：产品的性能任务及任务阶段、环境条件、工作原理、结构组成、试验和使用要求等	可以确定 FMECA 工作的深度和广度；为设计 FMECA 工作提供支持
		从生产工艺技术规范中获取：生产流程、工序目的和要求等	为过程 FMECA 工作提供支持
2	设计图样及有关资料	从设计图样可获取初始约定层次产品直至最低约定层次产品的结构、接口关系等信息	在设计初期的工作原理图可进行功能 FMECA；详细设计图样为硬件及软件 FMECA、DMEA 提供支持；生产工艺设计资料为进行过程 FMECA 提供支持
		从生产工艺设计资料获得生产过程的流程说明、过程特性矩阵，以及相关工艺设计、工艺规程等信息	
3	可靠性设计分析及试验	从产品可靠性设计分析及试验资料中获取故障信息或数据；当无试验数据时，可从某些标准、手册、资料中（如 GJB/Z 299《电子设备可靠性预计手册》）和软件测试中获取故障信息或数据	为设计 FMECA 的定性、定量分析提供支持
		从生产工艺，可获得包括生产过程中的故障模式、影响及风险结果	为过程 FMECA 进行定性、定量分析提供支持
4	过去的经验、相似产品的信息	从产品在使用维修中获取：检测周期、预防维修工作要求、可能出现的硬件/软件故障模式（含损坏模式）、设计改进或使用补偿措施等	为设计 FMECA、过程 FMECA 工作的开展提供支持
		从相似产品中获取有关 FMECA 信息	

应全面而广泛地收集、分析、整理有关被分析对象的相关资料，以作为进行 FMECA 的信息输入。

9. FMECA 工作的分工及职责

FMECA 工作应由产品设计人员或工艺设计人员完成，即“谁设计、谁分析”。可靠性专业人员应协助设计人员完成分析工作，提供实施 FMECA 的程序、方法，并进行指导与会签。应明确装备总体单位和配套单位之间的工作接口关系。FMECA 工作应分工明确，责任到人，严格实行岗位责任制。

10. FMECA 报告

FMECA 报告的主要内容一般包括以下几个方面：

- 概述——实施 FMECA 的目的、产品所处的寿命周期阶段、分析任务的来源等基本情况；实施 FMECA 的前提条件和基本假设的有关说明；编码体系、故障判据、严酷度定义、FMECA 方法的选用说明；FMECA、CA 表选用说明；分析中使用的数据来源说明；其他有关解释和说明等。
- 产品的功能原理——被分析产品的功能原理和工作说明，并指明本次分析所涉及的系统、分系统及其相应的功能，并进一步划分出 FMECA 的约定层次。
- 系统定义——被分析产品的功能分析、绘制功能框图和任务可靠性框图。
- 填写的 FMEA、CA 表的汇总及说明。
- 结论与建议——除阐述结论外，对无法消除的严酷度为 I、II 类单点故障模式或严酷度为 I、II 类故障模式的必要说明，对其他可能的设计改进措施和使用补偿措施的建议，以及预计执行措施后的效果说明。
- FMECA 清单——根据 FMECA 表的结果确定：“严酷度 I、II 类单点故障模式清单”及“可靠性关键重要产品清单”。
- FMEA、CA 表；危害性矩阵图等。

上述列出的报告内容，可根据工程需求，进行剪裁，视情况而定。

11. FMECA 的评审

应对 FMECA 的结果和报告进行评审。评审可结合产品研制转阶段节点评审或其他技术评审进行，也可以进行 FMECA 单项评审。

FMECA 是有效的可靠性分析方法，但在分析过程、评审中还应与其他可靠性分析方法相结合，例如与故障树分析（FTA）、事件树分析（ETA）等方法相结合。

5.7.5 FMECA 相关技术标准状况

1. 美国的 FMECA 标准

美国军方最早研究并制定了 FMECA 技术标准, 于 1949 年发布了 MIL-P-1629 《实施 FMECA 分析程序》。1950 年, 美国格鲁门 (Grumman) 公司针对新型喷射引擎 (Jet Engine), 为了评估其操纵系统的可靠度而使用了 FMEA 分析方法。随后在 20 世纪 60 年代早期, 美国国家航空航天局 (NASA) 要求其承制方开始运用 FMECA 工程技术, 在 1966 年, NASA 发布了用于阿波罗项目的 FMECA 程序。与此同时 FMECA 也扩展到民用航空领域, 1967 年 SAE 发布了第一个民用的 FMEA 标准——ARP 926 《Fault/Failure Analysis Procedure》。1974 年, 美国海军出版军用标准 FMEA 程序 MIL-STD-1629 (Ship) 代替 MIL-P-1629。1977 年, 美国海军航空系统司令部 (NAVAIR) 发布了 MIL-STD-2070 (AS), 1980 年美国海军发布 MIL-STD-1629A 代替了 MIL-STD-1629 (Ship) 和 MIL-STD-2070 (AS)。

1994 年 6 月, 美国国防部长佩里发布名为“规范和标准—采购的新方法”备忘录, 该备忘录要求国防部要更多地依赖民用产品和实践, 由备忘录产生的结果是大量的可靠性标准被删除, 其中也包括 MIL-STD-1629A, 并将更新 FMECA 工作程序的责任转移至 SAE, 2001 年 SAE 发布非汽车工业的 FMECA 的建议实践 ARP5580 《非机动车用的故障模式和效果分析的推荐实施规范》, 但是在军工和航天领域 MIL-STD-1629A 仍然有非常广泛的应用, 也不乏军工产品采用民用标准, 由于标准的选择变得复杂, 国防部下属的一些机构针对自身产品的特点发布了一些技术手册和指南, 如美国陆军部 2006 年发布的设计 FMECA 分析工作的技术手册, 美国空军航天司令部太空与导弹系统中心于 2009 年发布宇宙飞行器 FMECA 指南, 这些手册和指南能够更好地指导 FMECA 的实施。

2. 欧洲等地区的 FMECA 标准

除美国以外, 欧洲国际电工委员会 (IEC) 也在 1985 年发布 IEC 812 《系统可靠性分析技术——故障模式影响分析程序》(现在的 IEC 60812), 介绍了 FMEA 和 FMECA 的一般性使用, 基于同一目的, 英国标准协会 (BSI) 在 1991 发布了 BS 5760-5 《系统, 设备, 组件可靠性——故障模式, 影响和危害度分析》, 该标准借鉴了汽车行业的最佳实践, 将 FMECA 应用到工艺过程的设计中。

3. 汽车行业等民用 FMECA 标准

在民用行业, 福特汽车在 20 世纪 70 年代经历 Pinto 牌汽车的问题之后, 出于对安全性和法规遵守的考虑, 开始在企业内部导入 FMEA。



20 世纪 80 年代以后,许多汽车公司开始发展内部的 FMEA 方法,采用 RPN 风险分析方法评价潜在故障。这种风险分析方法与传统的美军标危害性分析方法有所差别。随后汽车业更将 FMEA 方法应用到工艺过程上,针对分析对象之不同,汽车业建立《设计失效分析 DFMEA》与《过程失效分析 PFMEA》两套程序,并开始要求零件供货商采用 FMEA 来分析所生产零件的设计与制程。由于各汽车公司的规定不尽相同,却纷纷被要求推行 FMEA,零件供货商的负担额外沉重,为改善这种现象,在美国品管学会(ASQC)的赞助下,北美三大汽车公司 Ford、Chrysler、General Motor 等组成的 AIAG,致力于整合各汽车公司规定的表格;在 1993 年,历经数年的努力后,AIAG 终于完成《潜在失效模式与影响分析参考手册》。借助此份手册的指导,汽车工业统一了失效分析的程序与表格,并且奠定了 FMEA 在工业界的地位,直到现在已经更新到 2008 年的第 4 版;三大汽车公司并没有就此止步,它们还通过标准体系的认证来促使供应商实施 FMEA,1994 年在 QS 9000 第一版的质量体系要求条款中,就加入了 FMEA 的要求,成为获得 QS 9000 认证的必要条件,随后也成为国际汽车行业的技术规范 TS16949《质量管理体系——汽车行业生产件与相关服务件的组织实施 ISO 9001:2000 的特殊要求》。

与此同时,一些行业协会也发布了自己的汽车业标准。1995 年,基于 AIAG FMEA-2《潜在失效模式与影响分析参考手册》内容,形成了 SAE 的 FMEA 正式技术文件 SAE J-1739《设计中的潜在失效模式影响分析和制造,或组装过程中的失效模式影响分析》,并与 AIAG 参考手册同步更新,在质量体系认证中,两者是可以等效的,最新的版本是 2009 年发布的。

4. 国内 FMECA 标准

20 世纪 80 年代初期,在引进、消化、应用和总结的基础上,相继发布了一系列有关 FMECA 的国家标准、军用标准、行业标准和指令性文件。

1985 年 6 月,由国家标准局颁发了国家标准 GJB 7826-87《系统可靠性分析技术失效模式和效应分析(FMEA)》,该标准能应用于不同产品(电的、机械的、液压传动装置等),以及由多种技术基础组合成的各种系统,还可用于软件和人类行为的研究。

1989 年 12 月,原航空工业部发布了航空标准 HB 6359-89《失效模式、影响及危害性分析程序》,该标准使用于航空产品的研制、生产和使用阶段,不适用于软件。

1992 年 7 月参考 1629A 发布了 GJB 1391-92,此标准的适用范围有限,规定了对产品进行故障模式、影响及危害性分析(FMECA)的要求和程序,仅适用于产品的研制、生产和使用阶段,不适用于软件 FMECA。为了跟上型号装备的要求,在 2006 年升级为 GJB/Z 1391-2006《故障模式、影响及危害性分析指南》,适用阶段由原来的研制、生产和使用,扩展为论证、方案、工程研制与定型、生产和使用,将

FMECA 分为设计 FMECA (含功能 FMECA、硬件 FMECA、嵌入式软件 FMECA 和 DMEA) 和过程 FMECA 两类, 并且增加了风险优先数的分析方法, 还增加了嵌入式软件 FMECA 方法、过程 FMECA 方法等内容, 相比 GJB 1391-92 版本, 更加全面地覆盖了武器装备型号的要求, 是目前国内军用产品应用中最广泛的标准。

1995 年 12 月, 原航空工业总公司发布了航空标准 HB/Z 281-95《航空发动机故障模式、影响及危害性分析指南》, 该标准使用于航空发动机的本体结构及其系统的研制生产和使用阶段, 但不适用于软件。针对航空发动机的特点, 对 GJB 1391 系列标准进行了剪裁和补充, 该标准提供了航空发动机所属产品的故障模式信息, 有助于航空发动机进行 FMECA。

纵观国外的 FMECA 标准发展情况, 国外的各种 FMECA 标准设计范围比较广泛, 既有军用的 MIL-STD-1629A, 也有民用的 QS 9000 (汽车制造行业); 涉及的 FMECA 方法也很多, 发展更早, 应用更广泛。其主要特点包括:

- 包含了丰富的基础数据。针对 FMECA 工作, 不仅提供了相应的 FMECA 分析流程、方法和表格, 还有丰富的基础数据作为 FMECA 的基础。
- 注重 FMECA 工作与其他工作的协调。由于起步早, 发展快, 应用广, 其工作更注重的是团队合作、协同管理, 在进行 FMECA 分析的同时, 考虑了可靠性、维修性、保障性等设计分析工作相协调, 达到数据共享, 并提高了工作效率。
- 国外的标准更体现、强调了管理的作用。在 QS 9000 等标准中, 强调在产品开发各阶段中, 需要通过不停地迭代更改, 发现产品的问题并进行质量改进, 提高产品的质量特性, 这些工作都是通过严谨的管理实现的。

相比之下, 国内的标准有很多不足之处, 大致体现为: 缺乏充分的基础数据, 包括故障模式库等, 严重影响 FMECA 工作的效果。FMECA 工作缺乏与其他工作的协调, 不够有效地利用已有的经验和数据, 例如, 对约定层次的划分和定义比较随意, 没有考虑与其他工作的协调处理。没有强调 FMECA 的管理工作, 这也体现了国内军工单位的管理水平及对 FMECA 的重视程度不够, 直到 2006 年才增加了软件 FMECA 及过程 FMECA 工作要求, 并且没有强调动态管理方面的内容, 因此国内开展 FMECA 工作与国外有较大差距, 在理论依据、数据基础、重视程度等方面, 都滞后于西方发达国家。

5. 几个重要 FMECA 标准介绍

目前国际上广泛应用的 FMECA 标准如表 5-16 所示, 主要有国际标准 (如 IEC 发布的标准)、国家级标准 (如 MIL-STD-1629 和 BS 5760-5)、行业性标准 (如 SAE 和 AIAG 发布的标准、美国国防部下属机构发布的技术手册) 等。

表 5-16 几个重要的 FMECA 标准

FMECA 标准	发 布 者	范 围
MIL-STD-1629A	美国国防部（DOD）	主要是包含功能 FMECA、硬件的 FMECA
SAE ARP 5580	机动车工程师学会（SAE）	非汽车工业的包括（功能\接口\硬件）FMECA、软件（功能接口\Detail）FMECA、过程的 FMECA
SAE J1739	机动车工程师学会（SAE）	设计 FMEA、工艺 FMEA 和设备 FMEA
AIAG FMEA-4	汽车工业行动小组（AIAG）	包括设计 FMEA 和工艺 FMEA
C4ISR 设备 FMECA	美国陆军部	设计 FMEA
航天器 FMECA 指南	美国空军太空司令部太空与导弹系统中心	功能 FMECA、硬件 FMECA 和接口 FMECA
BS 5760-5	质量管理与统计标准政策委员会	设计 FMECA 和过程的 FMECA
IEC 60182	国际电工委员会（IEC）	设计 FMECA 和过程的 FMEA
GJB/Z 1391-2006	中国国家科学技术委员会	功能 FMEA、硬件 FMECA、过程 FMEA、软件 FMEA

以下对这些技术标准进行简要介绍。

（1）MIL-STD-1629A（失效模式，影响及危害性分析）

目前的版本是 1980 年 11 月 24 日发行的 A 版，共有 57 页。该标准说明了如何执行 FMECA，详细叙述建立模式的方法、功能方块图、定义严重等级与危害性度量，提供一份 FMEA、危害性分析、FMECA—维修性信息表，以及损伤模式与影响分析单的样本表格，并且附有一些案例。

（2）SAE ARP 5580（非机动车用的故障模式和影响分析的推荐实施规范）

目前的版本于 2001 年 7 月发布，共 58 页。《SAE ARP 5580 非机动车应用的故障模式和效果分析的推荐实施规范》主要描述了实施 FMEA 的基本程序，包括功能、接口、详细（Detailed）FMEA，还包括一些分析前的工作（FMEA 计划和功能需求分析）、分析后的工作（潜在故障分析、FMEA 的验证、文件管理），以及在硬件、软件、过程设计中的应用。主要应用对象是那些希望在产品研发过程中使用 FMEA 作为一个工具来评估系统单元的安全性和可靠性，或者作为其产品改进过程中的一部分组织。

（3）SAEJ1739（设计中的潜在失效模式影响分析，制造和组装过程中的失效模式影响分析）

目前的版本是于 2009 年 1 月发布，本标准主要描述了设计中的潜在失效模

式、后果分析 (DFMEA) 和潜在故障在制造和装配过程中的模式和后果分析 (PFMEA)。通过提供适当的术语、要求、排列图表和工作表, 帮助用户识别减轻风险。作为一个标准, 文件中包含要求“必须”和建议“应该”, 以指导汽车工业用户展开 FMEA 过程。汽车工业的 FMEA 过程和文件, 必须符合这个标准, 以及任何这方面的企业政策标准。该标准与 AIAG FMEA-4 具有同等效力。

(4) AIAG FMEA-4 (潜在故障模式影响分析参考手册)

目前的版本于 2008 年发布, 标准主要阐述了设计故障模式影响分析和工艺故障模式影响分析, 提供了相应的表格和应用技术的一般性指南, 介绍了功能图、边界图、P 图等 FMEA 分析的辅助性工具, 这些方法对于军工行业也有很好的借鉴意义。

(5) C⁴ISR FMECA (C⁴ISR 设备的故障模式影响分析)

这是由美国陆军部于 2006 年公开发布的 FMEA 技术手册, 该手册的目的就是要通过故障模式、影响和危害分析 (FMECA) 的过程引导设备经历, 指导如何应用这种类型的分析方法运用到指挥、控制、通信、计算机、情报、监视和侦察 (C⁴ISR) 的设备中。这些设施包含了很多冗余系统, 用于实现极高的可用性。本手册在 1629A 的基础上详细描述了 FMECA 的分析流程, 同时也借鉴了汽车工业 FMEA 分析的实践, 引入了 RPN 的风险评价方法。

(6) Space Vehicle FMECA Guide (航天器 FMECA 指南)

这是由美国空军太空司令部太空与导弹系统中心于 2009 年发布的技术手册, 美国国家的太空项目 (包括航天器和发射运载工具项目) 经常发现很多关键故障、单点故障、非预期的故障影响, 以及相关的系统可靠性的降低, 在寿命周期的后期 (测试与集成阶段或者在轨阶段) 才被发现, 因此成立了任务保证改进 FMECA 小组, 讨论制定了本指南, 指南只包含硬件设计的 FMECA (功能 FMECA、硬件 FMECA、接口 FMECA), 为如何计划和执行一个详细的无人航天器, 以及与航天器存在接口的地面支持电子设备和地面支持机械设备 FMECA 提供指引。

(7) BS 5760-5 (系统/设备/组件可靠性——故障模式影响和危害性分析)

该标准是在英国国家标准局质量、管理及统计标准委员的指导下, 基于 IEC812 标准的内容修改完成的。该标准于 1991 年发布, 并成为系统、设备和元件可靠性标准体系第 5 部分的内容。本标准主要描述了 FMEA 和 FMECA, 并且如何应用它们来研发可靠的产品设计, 包括:

- 描述执行分析的程序。
- 提供合适的术语, 假设和故障模式及危害度度量。



- 确定基本的准则。
- 提供必要的工作表例子，包括设计和工艺的 FMECA。
- 提供应用 FMEA 和 FMECA 的建议。

(8) IEC 60182 (系统可靠性分析技术——故障模式影响分析程序)

最新的版本是 2006 年发布的，该版本是在 IEC 812 的基础上进行修订的，包含设计和工艺的 FMECA，广泛应用于汽车行业的 FMEA 分析方法，增加了更多的例子用于说明分析方法，提供了各种不同 FMECA 分析方法优劣的说明，阐述了 FMECA 与故障树分析的关系。

(9) GJB/Z 1391A-2006 (故障模式影响及危害性分析程序)

在 1992 年，中国发布 GJB 1391-1992《故障模式影响及危害性分析程序》，该标准基于 MIL-STD-1629 为原型编制，内容基本与 MIL-STD-1629 相同，在中国航空、航天、兵器、船舶等武器装备行业得到了广泛的应用。2006 年，对标准进行了修订，补充了工艺 FMEA 和软件 FMEA 技术内容，并对 FMECA 中的风险分析和控制方法进行了极大的改进。

5.8 故障树分析

5.8.1 故障树分析概念

故障树分析法 (Fault Tree Analysis) 简称 FTA。1961 年美国贝尔实验室沃森 (Watson) 等人在民兵导弹发射控制系统中开始应用，其后波音公司对 FTA 进行了修改，使其能用计算机进行处理，推动了 FTA 技术的迅速发展。FTA 现已成为分析各种复杂系统可靠性的重要方法之一。

故障树分析，是把系统不希望发生的故障状态作为故障分析的目标，这一目标在故障树分析中定义为“顶事件”。在分析中要求寻找出导致这一故障发生的所有可能的直接原因，这些原因在故障树分析中称之为“中间事件”。再跟踪追迹找出导致每一个中间事件发生的所有可能的原因，循序渐进，直至追踪到对被分析对象来说是一种基本原因为止。这种基本原因，在故障树分析中定义为“底事件”。

故障树分析法是自结果——不希望发生的顶事件（上级事件）向原因方面（下级事件）做树形图分解，是自上而下进行的。由顶事件起经过中间事件至最下级的基本事件用逻辑符号连接，形成树形图，再计算不可靠度（不安全概率）。

故障树建造是故障树分析的关键，也是工作量最大的部分。由于建树工作量大，因而这种方法在新的复杂系统上的使用受到局限。例如，美国原子能委员会发

表的 WASH-1400 核电站风险评价分析报告指出,为了建造故障树,60 名专家用了将近 3 年时间,消耗了大量资金。为此,国内外一些企业或科研机构,研发了相应的故障树分析工具,借助这些故障树分析工具,可有效减少构建故障树的工作量,提高工作效率。

在 FTA 中,应用布尔代数等按树形图逻辑符号将树形图简化,求最小割集(最重要的、致命原因事件的组合)并计算顶事件发生概率。与 FMEA 相比,不仅可以分析部件错误,还可以分析由于人员差错、软件错误、控制错误、环境应力等引起的故障,并可进行多重故障分析,可以从逻辑上明确故障的发生过程,定量计算顶事件的发生概率。

5.8.2 FTA 发展及应用

在 20 世纪 60 年代,人们对系统进行可靠性分析时,主要采用的方法是先画出可靠性框图,再用“布尔真值表”或“概率图法”进行分析。采用这种方法虽能给出系统正常工作到某一特定时刻的概率,但如果要进一步分析是什么原因使系统产生故障,或者要分析究竟哪个原因是主要的,则上述方法就显得不够了。另外,当系统比较复杂、元部件数量大时,用“布尔真值表”或“概率图法”实际上已经不切实际。然而在同一时期,随着科学技术的发展,迫使人们对这些复杂系统的可靠性、安全性做出评价。FTA 法就是在这种情况下应运而生的。

故障树分析(FTA)技术是美国贝尔电报公司的电话实验室于 1962 年开发的,它采用逻辑的方法,形象地进行危险的分析工作,特点是直观、明了、思路清晰、逻辑性强,可以做定性分析,也可以做定量分析,体现了以系统工程方法研究安全问题的系统性、准确性和预测性,它是安全系统工程的主要分析方法之一。一般来讲,安全系统工程的发展也是以故障树分析为主要标志的,为预测导弹发射的随机失效概率做出了贡献。1965 年波音公司在系统安全年会正式发表了 FTA,引起科技人员的重视和应用,其后,波音公司研制的 FTA 计算机程序,进一步推动了它的发展。FTA 很快从宇航范围进入核工业和其他领域。1974 年美国原子能委员会发表了关于核电站危险性评价报告,即“拉姆森报告”,该报告的成功之处在于应用了事件树和故障树分析法。它用这两种分析方法计算出初因事件的发生概率、工程安全设施故障概率,以及各种水平的放射性物质排入环境的事故概率,第一次定量地给出了核电站可能造成的风险,在和其他能源造成的风险以及社会现有其他设施的风险比较之后,令人信服地导出了核能是一种非常安全的能源的结论,大量、有效地应用了 FTA,从而迅速推动了它的发展。

从那以后,FTA 从航天、核能进入一般电子、电力、化工、机械、交通乃至土

木建筑领域。科学工作者和工程技术人员愈来愈倾向于采用 FTA 作为评价系统可靠性和安全性的手段,用 FTA 来预测和诊断故障,分析系统的薄弱环节,指导运行和维修,实现系统设计的最优化,从而 FTA 在全世界受到普遍重视。

在单调关联求最小割集的算法方面,1971 年 S.N.Semanderes 提出了由底事件向上进行布尔代数展开的上行法。1972 年 J.B.Fussell 和 WE.Veselg 利用与门仅增加割集容量、或门仅增加割集数目的原理提出了下行法,并应用到 MOCUS 程序中。1985 年 D.R.Shier 和 D.E.Whited 提出了反演法。W.UQuine 根据奎因原理,利用对合运算提出了合取法。R.J.Nelson 根据尼尔逊原理通过对布尔代数和进行两次补运算提出了双取补法。1978 年 H.Ku mamoto 和 E.J.He nley 在尼尔逊原理变形的基础上,借助二叉搜索树提出了 K-H 算法。1981 年 M.O.Locke 综合应用模块化、逆变换和合运算提出了洛克斯算法。在求顶事件发生概率方面,通常采用的是将最小割集用直接法或递归法,由相交和化为不交和来求解。1986 年 B.P. Lavon 提出了不借助割集的自顶向下的迭代算法。1998 年闻利群提出了一种完全依赖于所要求精度的近似算法——精度取舍法,在“故障树快速成算系统”软件中得到实际应用,但要同时兼顾精度和时间。

20 世纪,FTA 在适航安全性方面也得到了广泛认可,是适航、安全性领域的一项重要技术、工具。例如,当功能危险分析识别失效状态之后,可将 FTA 用作 PSSA 的一部分,以确定可能引起每个失效状态的存在于较低层次的单个失效或失效组合,然后,从 FMEA 中获取 FTA 基本事件的失效率。利用故障树结构,自上而下进行事件发生概率分配,即将功能危险分析和初步系统安全性分析提供系统的事件发生概率指标,逐层往下分配到具体的分系统或单机。


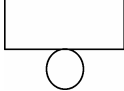






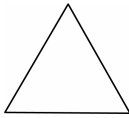




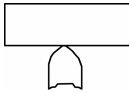
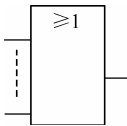

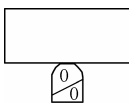
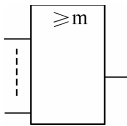
为了解决故障树烦琐的建树问题,以及如何应用故障树进行可靠性、安全性工作,2000 年工信部电子第五研究所开发的可靠性、维修性、保障性工程软件 CARMES 中的 FTA 模块提供了计算顶事件发生概率及事件重要度的容斥定理近似法、独立近似法及精确法,并在载人航天工程中得到了应用,2015 年发布的最新版本 CARMES 7 提供了基于模块化思想的算法,解决了复杂系统故障树计算效能的问题,并与安全性分析、可靠性框图、可靠性预计、FMECA 等方法紧密结合,实现了各分析工具之间的数据集成。这些可靠性工具的应用,将有效提高 FTA 的计算效率,大大节省分析时间。

5.8.3 FTA 中的图形符号



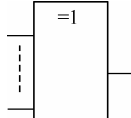

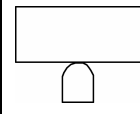
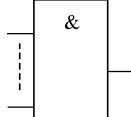

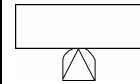

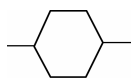

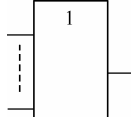
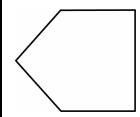
在 FTA 中建立故障树需要用到图形符号来表示事件或各种逻辑关系。不同的技术标准规定的故障树图形符号可能存在差异,IEC 61025 较详细地给出了这些符号

形式和说明，见表 5-17。

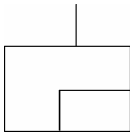

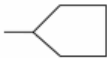

表 5-17 IEC 61025 推荐的故障树符号

符 号			名 称	说 明	与可靠性关系	输入事件数
			基本事件	其可靠性信息有效的最基本事件	零部件失效模式或一种失效原因	0
			条件事件	当两者都发生时顶事件才发生，其中一事件是另一事件发生的条件	一事件发生时另一事件发生的可能性	0
			潜在事件	表示潜在失效的初级事件；事件不能立即探明，但可能通过额外的检查或分析探明	零部件的潜在失效模式或失效原因	0
			未展开事件	表示系统中一部分还未展开的初级事件	与系统故障相关但其结构还未具体定义的系统部分	0
		 Transfer Out  Transfer IN 	转移门	表示系统此部分在图的其他部分或其他页展开	在整个系统中其他部分的可靠性框图	0
			或门	任何一个输入事件发生，输出事件就发生	串联系统的任何一部分发生故障，系统就失效	≥ 2
			多数表决门	如果多于 m 个输入事件发生，则输出事件就发生	对于 n 输入的 k 冗余系统， $m=n-k+1$	≥ 2

(续表)

符 号			名 称	说 明	与可靠性关系	输入事件数
			异或门	当且仅当一个输入事件发生时输出事件就发生	仅当一个可能的失效出现时，系统才失效	≥ 2
			与门	全部输入事件发生时，输出事件才发生	并联冗余	≥ 2
			优先与门	只有输入事件以从左到右的顺序发生时，输出事件才发生	适合表示二级失效或能排序的事件	≥ 2
			禁门	仅当两个输入事件发生，其中一个条件是条件，输出事件才发生	最终事件发生的条件概率	2
			非门	只有当输入事件不发生时，输出事件才发生	互斥事件或没有采取预防措施	1
			SEQ (顺序) 门	所有的输入事件按自左向右的顺序发生时，输出事件(故障)发生。如一些分析人员那样，如果输入 PAND 门的数量不限于 2，则此门等同于 PAND 门	适宜表示有顺序的故障(链式故障)。也适宜表示导致事件或故障发生的应力顺序。需要马尔科夫分析	>2

(续表)

符 号			名 称	说 明	与可靠性关系	输入事件数
			备用门	备用零部件的数目少于需要的数目时，输出事件将发生	表示冷、温和热各种备件，若它们全部服从指数分布，则存在解析表达式求解方法；若发生概率为常数，则需要马尔可夫分析；若为其他分布，则可能需要统计概率或仿真	≥1
			房形事件	已经发生或必将发生的事件		
			零事件	不能发生的事件		

5.8.4 故障树分析的一般方法与流程

1. 概述

故障树分析法是从所研究的故障现象（顶事件）出发寻找产生这一现象的根源，因而是从结果到原因，或是从上到下地研究系统或部件故障的方法。
故障树分析一般按下列步骤进行：

- ① 故障树的建造。
- ② 故障树的简化。
- ③ 定性分析。
- ④ 定量计算。
- ⑤ 确定改进措施。

2. 故障树的建立和简化

故障树建造是故障树分析的关键，也是工作量最大的部分。由于建树工作量大，因而这种方法在新的复杂系统上使用时受到局限。然而，对于某种性能渐变的故障分析来说，故障树分析是易于实现的，且比其他方法更加有效。
建树之前首先要熟悉对象，确定顶事件，用统一的标准符号表示树结构，对各事件进行编码。

**【例 5-10】某机舱内照明系统的故障树建立**

机舱内照明系统见图 5-26。通过分析，确定顶事件为：室内黑暗。分析各种故障因素，建立机舱内照明系统的故障树，见图 5-27。

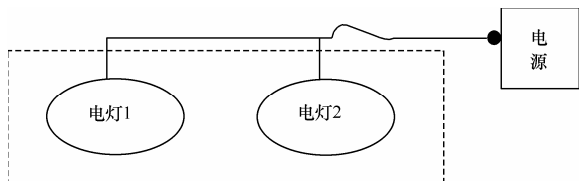


图 5-26 某机舱内照明系统图

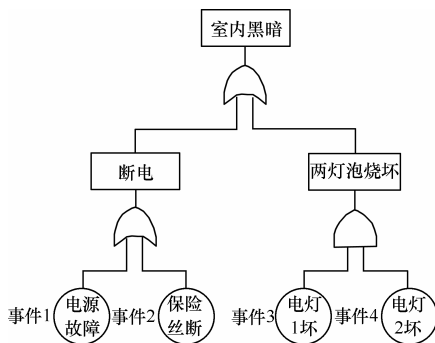


图 5-27 机舱内照明系统的故障树图

为了进行定量计算和处理共因事件，需要对已建好的故障树进行化简。简化可依据上级事件发生的必要条件进行，也可用布尔代数运算进行。

在进行故障树分析、计算时，需要用到布尔代数运算。下面是常用的布尔代数运算法则：

- ① 幂等律： $X+X=X$ $X \cdot X=X$ 。
- ② 加法交换律： $X+Y=Y+X$ 。
- ③ 乘法交换律： $X \cdot Y=Y \cdot X$ 。
- ④ 加法吸收律： $X+(X \cdot Y)=X$ 。
- ⑤ 乘法吸收律： $X \cdot (X+Y)=X$ 。
- ⑥ 加法结合律： $X+(X+Z)=(X+Y)+Z$ 。
- ⑦ 乘法结合律： $X \cdot (Y \cdot Z)=(X \cdot Y) \cdot Z$ 。
- ⑧ 加法分配律： $X \cdot Y+X \cdot Z=X \cdot (Y+Z)$ 。
- ⑨ 乘法分配律： $(X+Y) \cdot (X+Z)=X+(Y \cdot Z)$ 。
- ⑩ 摩根定理： $\overline{X+Y+Z}=\overline{X} \cdot \overline{Y} \cdot \overline{Z}$ 。
- ⑪ 摩根定理： $\overline{X \cdot Y \cdot Z}=\overline{X}+\overline{Y}+\overline{Z}$ 。
- ⑫ $(X+\overline{Y}) \cdot Y=X \cdot Y$ 。
- ⑬ $(X \cdot \overline{Y})+Y=X+Y$ 。
- ⑭ 互补定理： $X+\overline{X}=I$ ， $X \cdot \overline{X}=0$ 。
- ⑮ 常数运算定理： $X+0=X$ ； $X+I=I$ ； $X \cdot 0=0$ ； $X \cdot I=X$ 。

其中， I 为全集， 0 为空集。

采用布尔代数进行运算化简的主要方法如下。

(1) 全为 AND 门

全为 AND 门时 (如图 5-28 所示), 无论多么复杂的分支, 其全部基本事件都可以输入到一个 AND 门下。如果这时有同一基本事件出现在两处以上, 也可以化简成一处。用布尔代数运算可表示为:

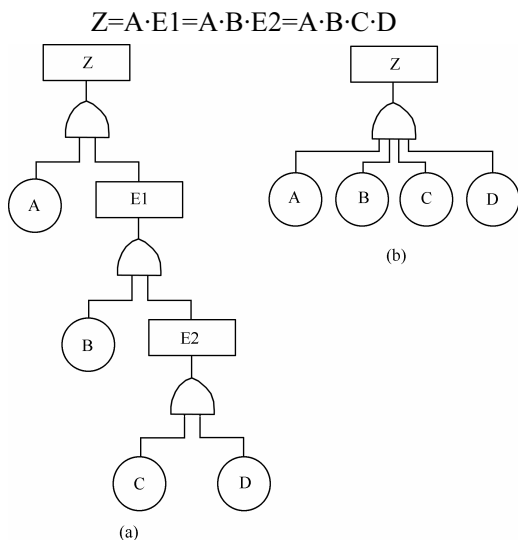


图 5-28 全为 AND 门时故障树化简

(2) 全为 OR 门

全为 OR 门时 (如图 5-29 所示), 无论多么复杂的分支, 其全部基本事件都可以输入到一个 OR 门下。如果这时有同一基本事件出现在两处以上, 也可以化简成一处。用布尔代数运算可表示为:

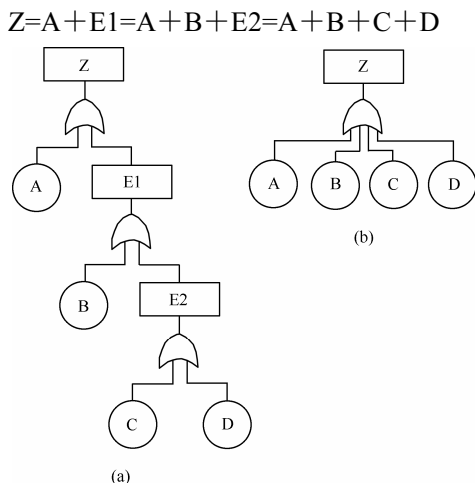


图 5-29 全为 OR 门时故障树化简

(3) 有共因事件时的简化

共因事件时的化简目的是为了减少定量计算的错误，如图 5-30 所示的故障树，其共因事件的简化方法如下。

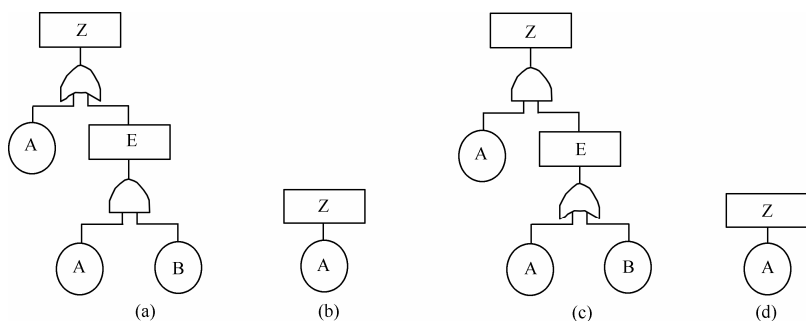


图 5-30 有共因事件时的故障树化简

对于图 5-30 (a) 中的故障树，应用加法吸收率可得：

$$Z=A+E=A+(A \cdot B)=A$$

对于图 5-30 (c) 中的故障树，应用乘法吸收率可得：

$$Z=A \cdot E=A \cdot (A+B)=A$$

结果都消除了重复的 A。

3. 定性分析

FTA 的主要目的是要找出顶事件发生的路径或机理并加以评判，从而为改善系统采取措施。为了有效地进行这项工作，需要求出故障树的最小割集。

(1) 最小割集

设故障树中含有 n 个底事件： X_1, X_2, \dots, X_n 。 $C_i=\{X_{i1}, X_{i2}, \dots, X_{im}\}$ 为其中某些底事件组成的一个集合，若集合中的事件都发生时，顶事件必然发生，就把 C_i 称为故障树的一个割集。若 C_i 是一个割集，且在 C_i 中任意去掉一个事件后就不再是割集，则 C_i 是一个最小割集（简称 MCS）， C_i 中的事件个数称为该最小割集的阶数。

求最小割集的方法很多，最常用的有上行法和下行法。对比较简单的系统，一种简易的方法是：从垂直于可靠性框图中连接实线的方向，将系统单元的功能切断（使之处于故障状态）时引起系统故障的被切单元的最小集合。

MCS 是导致顶事件发生的最少底事件的一种组合，可有效查找复杂系统的故障线索，对系统可靠性设计有重要作用。

(2) 定性分析概述

FTA 的首要任务是做好定性分析。定性分析的基本任务和作用是识别系统所有可能的故障模式，并按单元的重要性和 MCS 的阶数排列轻重次序。这对于发现系

统薄弱环节并采取有效预防或减缓措施，具有重要作用。

定性分析的主要工作内容就是查找 MCS 并进行分析比对。就 MCS 阶数而言，阶数越低的最小割集越重要；就底事件而言，在低阶 MCS 中出现的底事件较在高阶 MCS 中出现的同一底事件要重要；在相同阶数的 MCS 中，重复出现次数越多的底事件越重要。

4. 定量分析

故障树定量分析是定性分析的发展和延续。利用故障树进行定量分析时，需要计算顶事件的发生概率、结构重要度、概率重要度等参数。

一般而言，故障树的定量计算工作量较大，可借助相应的计算机辅助工具进行量化计算。

(1) 顶事件发生概率计算

顶事件发生概率的计算需要先求故障树的 MCS，是一个复杂的过程。简言之，顶事件可用故障树全体 MCS 的布尔表示。要计算顶事件的发生概率，需要将全体 MCS 进行不交化处理，化为两两互斥，再求不交积之和。

(2) 重要度分析

重要度是指当一个部件或者系统的割集发生失效时，对顶事件发生概率的贡献，是时间、部件的可靠性参数以及系统结构的函数。它在系统的可靠性预测、分配、运行、维修、储存管理中都起着指导性作用。例如：可以估计由部件可靠度参数的变化所导致的系统可用度的变化，可以按部件重要度的顺序进行检查、维修和发现故障，并改进重要度较大的部件，从而提高系统的可靠性。根据不同的情况，重要度有多种定义。如最早由 Birnbaum 提出的且在生产实际中被广泛应用的结构重要度 (Structural Importance) 和概率重要度 (Birnbaum Reliability Importance)；Lambert 提出了关键重要度 (Criticality Importance)；Fussell 和 Vesely 提出了 FV-重要度 (FV-Importance)；Butler 定义的一种仅依赖于路集和割集的部件重要度、不依赖于部件可靠度的 P-重要度 (Path Importance) 和 C-重要度 (Cut Importance)；Barlow 和 Proschan 提出的 B-P 重要度 (B-P Importance)；Pan 等介绍的蒙特卡罗方差重要度 (Monte-Carlo Variance Importance) 等。重要度在实际工程中得到了广泛的研究和应用，有助于有效地改进系统可靠度；对系统的运行提供有效的设计方法或寻找系统的失效原因等。

① 结构重要度。

工程实践表明，从可靠性、安全性的角度看，系统中各部件并不是同等重要的，因此，引入重要度的概念用以表明某个部件对顶事件发生的影响大小是很必要的。重要度是故障树分析中的一个重要概念，对改进系统设计，制订维修策略是十

分有利的。对于不同的对象和要求，应采用不同的重要度。

结构重要度指的是元部件在系统中所处位置的重要程度。它与元部件本身的故障率没有关系，如图 5-31 所示。结构重要度的计算过程如表 5-18 所示。

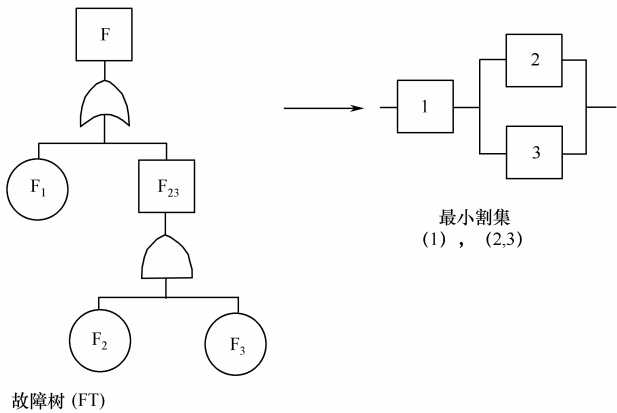


图 5-31 结构重要度计算示意图

表 5-18 结构重要度的计算过程

基本事件			系统	用 1 表示故障，用 0 表示正常	
1	2	3			
0	0	0	0	元素 1 正常，故障与状态数之比为 1/4	元素 1 的重要度为： $\frac{4}{4} - \frac{1}{4} = \frac{3}{4}$
0	0	1	0		
0	1	0	0		
0	1	1	1		
1	0	0	1	元素 1 故障，故障与状态数之比为 4/4	
1	0	1	1		
1	1	0	1		
1	1	1	1		

同理可得：

元素 2 的结构重要度为： $\frac{3}{4} - \frac{2}{4} = \frac{1}{4}$

元素 3 的结构重要度为： $\frac{3}{4} - \frac{2}{4} = \frac{1}{4}$

由于元素 1 为最小割集，所以其重要度最大，2、3 的重要度最小。

② 概率重要度。

概率重要度定义为某元素从故障状态变为正常状态时，系统的不可靠度改善了多少。因此，事先必须知道所有元素的可靠度。

$$F_{\text{系统}}(F_i=1) - F_{\text{系统}}(F_i=0) = \Delta F$$

以图 5-31 为例, 假设各元素的可靠度为 $R_1=R_2=R_3=0.9$; 元素 1 故障时, $F_1=1$, 则 $F_{\text{系统}}=1$; 元素 1 正常时, $F_1=0$, 则 $F_{\text{系统}}$ 等于元素 2、3 并联系统的不可靠度, 即:

$$F_{\text{系统}}=F_2 \cdot F_3=0.01$$

所以, F_1 的概率重要度为 $\Delta F_1=1-0.01=0.99$ 。

至此, 可计算得到图 5-31 中故障树的定量分析结果, 见表 5-19。

表 5-19 故障树定量分析的结果

基本事件	元素	结构重要度	概率重要度 (各元素可靠度为 0.9)
F_1	1	0.75	0.99
F_2	2	0.25	0.09
F_3	3	0.25	0.09

③ Birnbaum 结构重要度。

所谓 Birnbaum 结构重要度又称概率结构重要度, 它是指在只有第 i 个部件由正常状态变为故障状态时, 使顶事件发生概率的变化率, 其定义用下式表示:

$$I_i^{Pr}(t) = \frac{\partial g(Q(t))}{\partial Q_i(t)} = g(1_i, Q(t)) - g(0_i, Q(t)) \quad (5-38)$$

从数学意义上讲, Birnbaum 结构重要度是指顶事件发生概率对底事件发生概率的偏导数, 又可写成:

$$I_i^{Pr}(t) = E\{\Phi[1_i, X(t)] - \Phi[0_i, X(t)]\} = P\{\Phi[1_i, X(t)] - \Phi[0_i, X(t)] = 1\}$$

从数学定义上可以解释为: 第 i 部件的概率重要度就是 i 部件状态取 1 时顶事件概率和 i 部件状态取 0 值时顶事件概率值的差, 即部件 i 的概率重要度就是系统处于部件 i 为关键部件状态的概率。

④ 关键重要度。

所谓部件 i 的关键重要度是指底事件故障概率的变化率与由它引起顶事件发生概率的变化率之比。其定义用下式表示:

$$I_i^{Cr}(t) \equiv \lim_{\Delta Q_i(t) \rightarrow 0} \frac{\frac{\Delta g(Q(t))}{g(Q(t))}}{\frac{\Delta Q_i(t)}{Q_i(t)}} = \frac{Q_i(t)}{g(t)} \frac{\partial g(Q(t))}{\partial Q_i(t)} \quad (5-39)$$

因为:

$$I_i^{Pr}(t) = \frac{\partial g(Q(t))}{\partial Q_i(t)}$$

所以:



$$I_i^{Cr}(t) = \frac{Q_i(t)}{g(t)} I_i^{Pr}(t)$$

可见, 用概率结构重要度乘上因子 $\frac{Q_i(t)}{g(t)}$ 就可求出关键重要度。

⑤ Fussell-Vesely 部件重要度。

Fussell-Vesely 在研究部件重要度时, 发现只研究部件处于关键状态的重要度还不够, 还必须研究部件处于非关键状态时的重要度。所谓处于非关键状态是指当部件 i 由正常状态变为故障状态时, 顶事件并不发生, 但是部件 i 对顶事件发生的概率却有影响。

下面先介绍最小割集并集的概念: 假设包含第 i 个故障部件的全部最小割集数为 N_k^i (不一定是关键割集), 由它们构成的并集结构函数记做:

$$\Psi_k^i[X(t)] = \begin{cases} 1, & \text{含部件} i \text{的最小割集并集发生} \\ 0, & \text{含部件} i \text{的最小割集并集不发生} \end{cases}$$

则包含部件 i 的 N_k^i 个最小割集并集的结构函数为:

$$\Psi_k^i[X(t)] = \bigcup_{j=1}^{N_k^i} \bigcap_{l \in K_j} x_l$$

其概率 $g_k^i[Q(t)] = E\{\Psi_k^i[X(t)] = 1\}$ 为部件 i 对顶事件发生概率的贡献。

因此, 定义 FV 重要度为:

$$I_i^{FV}(t) = \frac{g_k^i[Q(t)]}{g[Q(t)]} \quad (5-40)$$

⑥ Barlow-Proschan (BP) 重要度。

所谓 (BP) 重要度是指部件 i 在过去一段时间里所发生的故障对顶事件发生概率的贡献。假设每一时刻 t 系统中只可能有一个部件发生故障, 部件 i 的故障密度为 $f_i(t)$, 则在 $[0, t]$ 区间内部件 i 发生故障导致顶事件发生的概率:

$$I_i^{BP}(t) = \int_0^t [g(1_i, Q(t)) - g(0_i, Q(t))] f_i(t) dt = \int_0^t V_{g_i} f_i(t) dt (\text{未归一化}) \quad (5-41)$$

I_i^{BP} 表示部件 i 在 $[0, t]$ 区间内发生故障对顶事件发生的累积贡献, 它是表示时刻 t 以前的事件, 而不是时刻 t 的事件。为了归一化, 也可将上式除以 $g(Q)$, 这时 $\sum_{i=1}^n I_i^{BP} = 1$ (归一化) 成立。

⑦ Fussell-Vesely 最小割集重要度。

Fussell-Vesely 最小割集重要度是表示最小割集发生时对顶事件发生的贡献。在时刻 t 最小割集发生概率与顶事件发生概率之比称为 FV 最小割集重要度, 即:

$$I_i^{*FV} = \frac{Q_i^*(t)}{Q_r(t)} = \frac{Q_i^*(t)}{g(Q)} \quad (5-42)$$

若需要进一步了解上述重要度的计算方法，可参阅相关文献资料。

5.8.5 共因故障问题

在建立故障树分析的过程中，共因故障是一个值得关注的问题。关于共因故障的定义，在 5.3.8 节已经介绍。鉴于共因故障事件对系统故障发生概率的影响很大，建立故障树时，需要慎重考虑系统是否存在共因事件问题。

若某个故障事件是共因事件，则对故障树的不同分支中出现的该事件必须使用同一事件标号。若该共因事件不是底事件，必须使用相同转移符号简化表示。一般说来，一个共因事件在同一系统故障树的不同子树中出现，这条规则往往可以得到遵守，但有时不同系统是相关的，比如共用同一电或水供应设施，设置共用同一个阀门或管路，而这两个系统由不同人建树，这条规则往往得不到遵守，从而导致错误。因此对一些大项目实施故障树分析时，技术负责人一定要采取妥当的措施以保证规则能得到遵守，比如让同一个人负责有相同共因事件的不同系统故障树建造工作。

5.8.6 动态故障树分析

动态故障树是在静态故障树的基础上，引入表征动态特性的新的逻辑门类型，例如优先与门、功能相关门、备件门、顺序相关门等。

动态故障树是指那些至少包含一个专用动态逻辑门的故障树。它把传统的故障树分析扩大到动态系统性能，基本上是静态故障树的一种扩展，具有顺序相关性、公用资源库、各种可修复系统，以及冷、热备件等特性。

与事件出现顺序相关的任何特性，都会影响系统的工作状态。例如：某系统在事件 A 和 B 结合起来时才导致系统失效，而与事件 A 和 B 出现的顺序无关时，它就是静态故障树；如果与事件 A 与 B 发生的顺序有关，必须是事件 A 首先发生，AB 结合才导致系统失效事件时，表明了事件发生的顺序相关性，这时就必须用动态故障树建模了。

传统的故障树模型涉及的逻辑门包括“与门”、“或门”、“表决门”、“非门”等。为了使故障树模型更好地处理特殊的与现今计算机应用系统有关的复杂特性，需要引入几种常用的典型动态逻辑门。

1. 优先与门 (PAND)

在容错系统的可靠性分析中，系统的故障模式不仅与基本事件的组合有关，而且与基本事件发生的先后顺序有关。这种特性可用优先与门来表征。优先与门在逻

辑上相当于与门，只是附加了一个条件：事件必须以指定的顺序发生。

2. 功能相关门（FDEP）

系统中某个部件的发生故障（称其为激发事件）可能会导致与其相关的其他部件无法进入工作状态或者发生故障。

3. 冷备件门（CSP）

假定系统具有冷备件（在激活工作之前不会失效的备件），这样的系统无法用标准的故障树技术建模，因为这样的故障树模式无法在同一个事件框架内用基本事件的组合进行表达。

4. 温备件门（WSP）

温备件门与冷备件门的不同之处在于温备件在进入工作状态之前具有大于零的失效率，而冷备件失效率为零。

5. 热备件门（HSP）

在某些可靠性要求较高的系统中，往往采用热备件（部件不论在运行或在储备，其失效率相同）随时切换到工作状态。若两个热备件门带有公用备件，则该备件可替换任意一个故障部件。

动态系统特性已不能简单地由底事件的组合表征，而必须考虑底事件发生的顺序关系以及部件之间的依赖关系。图 5-32 是一个动态故障树，其除了含有静态逻辑门外，还包含了动态逻辑门中的顺序门和冷备件门。

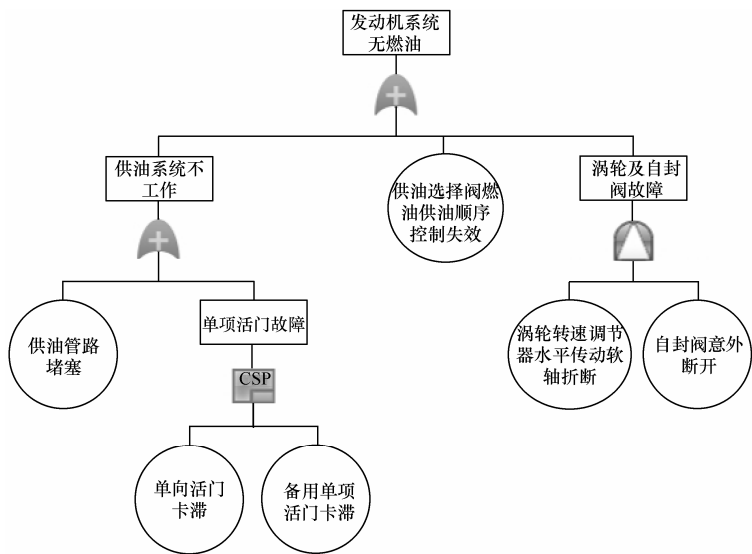


图 5-32 动态故障树示例

对于具有冷、热备件的系统,随着状态变化,其组件失效率变化是不连续的,冷备件在激活工作之前不会失效,温备件失效率较低,而热备件则始终具有较高的失效率,但冷备件和温备件在被激活进入工作状态之后同样具有较高的失效率,这反映了备件失效率与其所处状态密切相关而且其变化具有不连续性。

通常情况下,在整个故障树中只有很小的一部分在本质上是动态的,所以在用综合法对整个故障树进行处理时,首先要分辨出整个故障树中的独立子树,即由不在故障树其他位置出现的输入事件组成的子树。只含静态逻辑门的独立子树为静态子树,含有动态逻辑门的独立子树为动态子树。

5.9 潜在通路分析

5.9.1 潜在通路分析的内涵

潜在通路(Sneak Circuit)的概念最早是由美国波音公司在完成阿波罗登月计划期间,针对电子电气系统提出来的。波音公司通过对许多重大故障与事故案例的研究,发现有许多故障与事故并不是由于元器件失效引起的,而是由于系统设计方案之中固有的状态引起的。而这些状态是设计者为了实现设计意图而无意带进设计方案中的。同样,在复杂的气路、液路系统中也存在潜在路径(Sneak Path),软件系统也存在,这些潜在路径同样具有严重的危害,通常把潜在电路和潜在路径统称为潜在通路。

潜在分析是指确定在产品的所有组成部分均正常工作的条件下,能抑制正常功能或诱发不正常功能的潜在状态的一种分析技术,包括针对电路的潜在电路分析、针对液气管路的潜在通路分析、针对软件的潜在状态分析。

5.9.2 潜在通路的特点

潜在通路具有以下特点:

- 一种设计状态:虽然潜在通路发生时,往往表现为突发、难以理解等特点,但是它属于系统设计所固有的状态,只是因为潜在的激励条件或激励响应的因果关系难以识别,使得设计者忽略了这种状态的存在。
- 与元器件失效无关:也就是说,不考虑元器件损坏、参数飘移或偏离精度、环境变化等导致的系统失效或故障,而是考虑系统设计本身存在的“潜在通路”。
- 潜在通路难以通过试验发现,并具有潜伏性:多数潜在通路,并非每次运行都会起作用,必须具有发生作用的激励条件才能起作用。因此,多数情况



下，难以通过试验来发现潜在通路的存在。

- 复杂系统中可能大量存在潜在通路，而且往往难以避免：在复杂系统的电路设计、管路设计过程中，潜在通路几乎是难以避免的，必须采用潜在通路分析方法加以发现和改正。

5.9.3 潜在通路产生的原因

潜在通路产生的原因，主要包括以下 3 个方面：

1. 面条因素

这是指由于系统功能、结构、状态等的复杂性而形成的输入输出数据的错综复杂状态。复杂系统的功能路径与电气路径之间的相互“缠绕”，犹如一碗面条。产生“面条因素”的原因主要来自于系统及其相关设计资料的规模与复杂性。系统的多种数据（包括原理图、连接图、布线图等），均围绕设计加工为目的进行组织，因而各种性质、功能的信号在电路中相互交错和续接，客观上设计者难以清晰地把握系统全部可能的工作方式，容易在设计中无意引入潜在电路。

2. 洞视因素

对于型号研制任务细分的问题，大多数复杂的型号研制工作都是分级承包研制。设计工作的层次化分工，分系统设计人员对系统整体设计缺乏全面、深入的认识，对如何适当地连接各分系统缺乏全面的考虑。对设计评审后所做的更改将给各系统带来的影响未进行充分的审查。

3. 人的因素

人的因素主要有两个方面：

- 第一方面，设计人员设计出的产品不完全符合设计意图。不同的设计者对同一电路的不同理解可能导致不一致的系统人机界面。在特定的环境下，复杂的操作程序和设备实际状况之间的任何细小的差别，都可能导致操作者对系统真实状态做错误的判断，或在错误的时间向系统实施错误的激励。原理设计不能准确或完全反映设计意图、工程设计不能准确或完全反映原理或设计意图等。
- 第二方面，操作人员非期望的操作激发潜在电路。

5.9.4 潜在通路的表现形式

潜在通路的种类或表现形式主要包括下列 4 种：

- 潜在路径：物质流、能量流、数据流或逻辑信号流所流经的非期望路径。
- 潜在时序：物质、能量、数据或逻辑信号以非期望或矛盾的时间顺序，或在非期望的时刻，或延续一个非期望的时间段发生，从而使系统出现异常状态。
- 潜在指示：系统运行状况的模糊或错误的指示。潜在指示可能误导系统或操作人员做出非期望的反应。
- 潜在标志：系统功能（如控制、显示）的错误或不确切的标志。潜在标志可能会误导操作人员。

5.9.5 潜在通路分析技术现状

潜在通路分析技术，是一种有效识别安全关键系统、任务关键系统的潜在故障的有效手段，在航天、航空领域得到了应用。但是，由于该项分析技术的难度较大，至今可借鉴的分析工具、手段较少，一直以来这种分析技术更多依赖于经验以及设计师的专业知识进行判断。潜在通路分析技术的发展状态如下：

- 1960 年，美国红石火箭发射失败，在对事件的调查中首次发现了潜在通路问题。
- 1967 年底，波音公司在“阿波罗”计划中首次系统地开始了潜在通路分析工作，提出了潜在通路分析的概念。
- 至 20 世纪 80 年代，波音公司已经开发出适用于各类电路、机电系统以及软件系统的潜在分析技术，作为核心机密被称作“黑色艺术”。
- 自 20 世纪 80 年代中后期开始，SCA 技术进入航天和军工之外更广泛的领域，波音、ESA、美国 SoHaR 公司以及国内相关机构均开发了各自不同的 SCA 手段。

国外 SCA 设计分析技术逐渐趋于成熟，广泛应用于军民领域，可参见表 5-20。

表 5-20 美国 NASA 部分空间环境潜在电路分析项目情况

项目	设备/子系统要求	设备类型	研制阶段	分析类型	潜在问题数统计
“阿波罗”/ASTP(多级火箭)	电源分布控制，供电设备接口	继电器	全尺寸(FSED)	硬件、过程、任务支持、射流技术变化	208 SCR 13 DCR 1500 DER
天空实验室	电源控制，实验模块，供电设备接口	继电器	FSED	硬件、接地过程、任务支持、变化	259 SCR 307 DER

(续表)

项目	设备/子系统 要求	设备类型	研制阶段	分析类型	潜在问题数统计
“土星”1-C	电源控制, 供电 设备接口	继电器	大批量生产 (UP)	硬件	EPS: 7 DCR ESE: 20 DCR
“伯纳”II	飞行时序	继电器	FSED	硬件	2 SCR 4 DCR 6 DER
AST-F 应用技术 卫星	电源, 时序, 实 验, 遥测, 推力 控制	继电器, 数 字逻辑	全尺寸初样 研制	硬件、变化、过程	55 SCR 67 DER
航天飞机(多级 火箭)	全部子系统, 供 电设备接口	继电器, 数 字, 模拟, 微处理器	FSED	硬件、变化	124 SCR 85 DCR 728 DER
注: SCR—Sneak Circuit Report, 潜在电路报告; DCR—Design Concern Report, 设计缺陷报告; DER—Design Error Report, 设计图纸误差报告。					

国内一些型号主要在航天系统中得到应用, 如运载火箭、导弹、飞船、卫星等。
目前 SCA 的相关标准有:

- 1980 年, SCA 被列入美军标 MIL-SYD-785B 第 205 号工作项目。
- 1984 年, MIL-HDBK-338《电子设备可靠性设计手册》中介绍了 SCA 的种类、分析方法、软件 SCA 以及软硬件综合 SCA。MIL-STD-1543B《航天器和运载器可靠性大纲的要求》中对潜在通路的 4 种类型做了定义, 并给出了设计检查线索表和设计缺陷线索表。
- 1997 年, 欧洲空间标准化合作组织发布 ESCC-Q-40-04A, 规定了潜在分析的方法、程序和线索表。
- 2005 年, 我国发布航天行业标准 QJ 3217-2005《潜在分析方法和程序》。

在潜在分析软件工具方面, 国外应用较广的有美国波音公司的 ASP、欧洲航天局的 SNAP、美国 SoHaR 公司的 SCAT。我国的航天标准化与产品保障研究院、航天 12 所、工业和信息化部电子第五研究所等都开发了相应的潜在分析软件工具。

5.9.6 潜在通路分析方法与流程

1. 潜在分析工作概要

潜在分析工作, 一般是在电路图纸资料全部确定、投产之前进行分析。任务关

键系统、安全性关键系统是潜在分析的重点分析对象和范围。潜在分析的工作内容包括电路的潜在电路分析、液/气管路的潜在通路分析、软件的潜在分析。参与潜在分析的人员包括系统设计人员、待分析系统领域的专家、潜在分析的专家。在开展潜在分析工作时，需要注意以下几点：

- 要根据对可靠性、安全性的影响程度对复杂系统进行适当剪裁、划分。
- 潜在分析需要不断更新、反复，需要注重积累。
- 当元器件总数少（例如 < 50 个）的潜在分析，可用人工方法进行，但超过一定规模时，一般采用软件工具辅助进行。

2. 潜在通路分析方法

潜在通路分析方法主要包含基于拓扑模式识别和基于路径追踪两种。

（1）基于拓扑模式识别的分析方法

在基于拓扑模式识别的分析方法中，应用最为普遍的是基于网络树的方法。这是一种形式化的识别方法。

任何系统，无论是其结构复杂程度、系统各部件相互连接的关系复杂程度，总能够按照其物质流、能量流、数据流和逻辑信号流的传播模式，一般都能以网络树的形式表示系统各部件间的相互连接关系。网络树表达了系统中物质流、能量流、数据流和逻辑信号流传播的最重要的结构信息。

由于拓扑结构上相似的系统倾向于表现出相似的功能，因此可以通过对网络树进行拓扑识别，并利用事先建立的关于特定拓扑模式的线索表，识别系统所具有的功能。

以电子/电气系统为例，系统内各部件间相互连接关系的拓扑图，总是能够分解为下列5种基本的拓扑模式及其组合的形式，如图5-33所示。

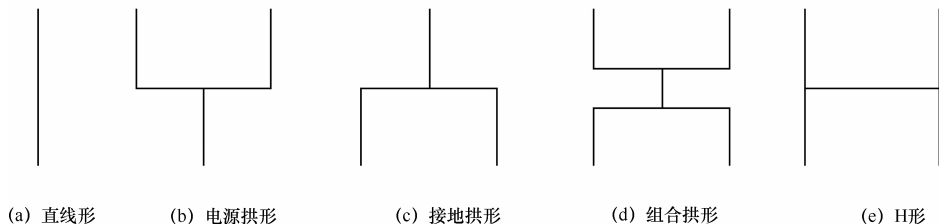


图 5-33 电子/电气系统的5种基本拓扑模式

基于网络树拓扑模式识别的分析方法的主要步骤包括：

- ① 对系统进行适当的划分以及结构上的简化，生成网络树。
- ② 根据图5-34识别网络树中的拓扑模式。

③ 结合线索表（一般是根据经验，判定特定拓扑模式下的潜在通路的指导性线索表）对网络树进行分析，识别出系统中存在的潜在状态。

波音公司所采用的 SCA 方法和工具，就是基于网络树拓扑模式识别。波音公司的 SCA 方法严格按数据采集、系统划分、数据输入、路径跟踪、网络树绘制和分析 6 个步骤进行。在实施 SCA 方法的过程中，需要网络树生成工具和专用的线索表。从波音公司的 SCA 方法可知，基于网络树拓扑模式识别的方法的优点是分析结果完整、准确，缺点是成本高、分析周期长、建立完善的分析程序和线索表难度大。

（2）基于路径追踪的方法

与基于拓扑模式识别的分析方法相比，基于路径追踪的识别方法更为简易。

基于功能节点识别和路径追踪的分析方法是：首先对复杂系统进行划分和简化；其次识别出系统中的功能节点，追踪出功能路径；最后结合线索表进行路径分析，识别出系统中存在的潜在状态。其中，系统中的功能节点可划分为源节点和目标节点两类。功能路径是指为完成系统的某项特定功能，系统内物质流、能量流、数据流或逻辑信号在功能节点间的传输路径。对于功能路径的识别一般是针对特定的源和目标进行的。

基于路径追踪的识别方法是欧空局（ESA）提出并采用的简化 SCA 方法。这种方法不需要画网络树，只需搜索源点到目标点的所有路径，并对这些路径应用两类线索进行潜在识别（路径线索、部件+路径线索）。设计缺陷分析依靠第三类线索进行（“部件”线索）。这种方法的优点是简化 SCA 操作，更早发现潜在问题，开支小，缺点是分析结果取决于三类线索的丰富程度，分析结果可能不全面，且这三类线索的建立，需要一定的积累和经验。

3. 潜在通路分析的一般程序

潜在通路分析可分为 3 个阶段：准备阶段、分析阶段和结论阶段，各阶段的主要工作及流程见图 5-34。

（1）准备阶段

准备阶段主要包含资料收集、消化和数据预处理。

应尽可能多地收集与待分析系统相关的资料，这些资料应准确、全面和有效。需要收集的资料包括：系统的设计任务书（或研制总要求）、相关的系统技术文件（含结构和功能框图、技术说明文件、系统电原理图、系统总布置图、电缆束的结构数据、各组成单机或部件的详细电原理图、系统定义中的“黑盒子”接口电路或等效电路数据、各组成单机或部件的内部接线表、元器件清单及相关信息、电连接器清单，以及相关信息和装配图等）。

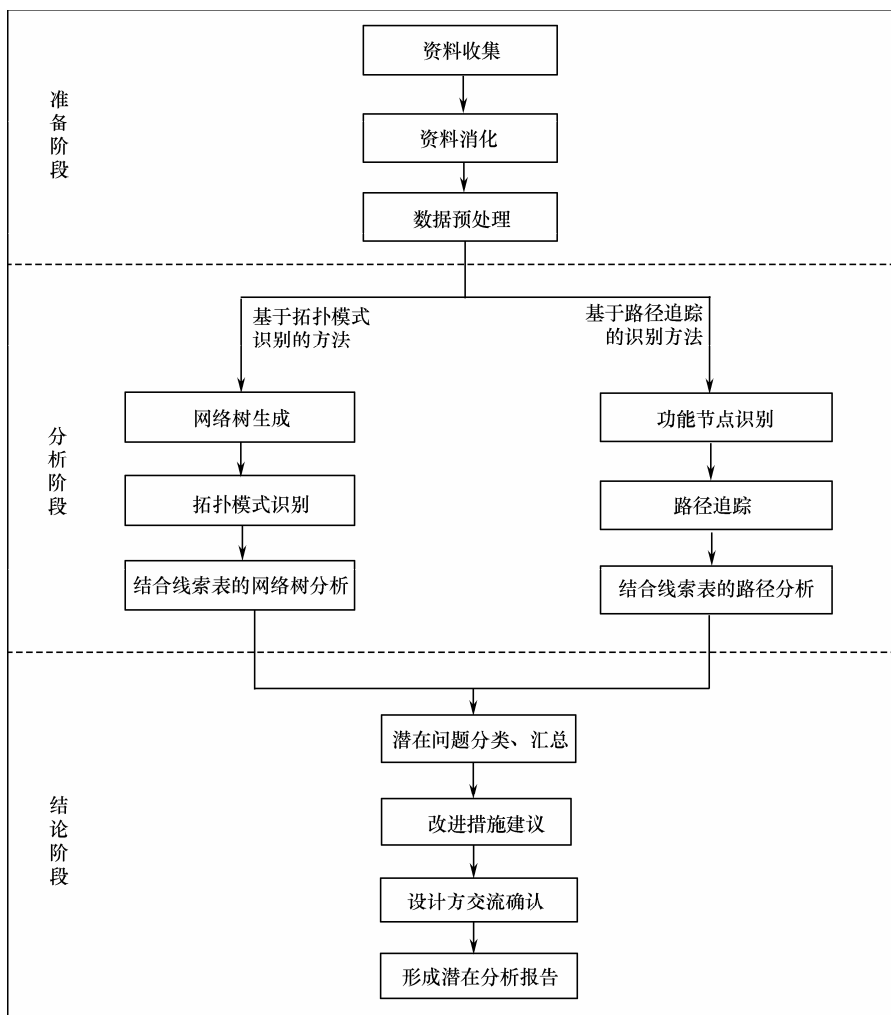


图 5-34 潜在通路分析的一般程序

然后，全面系统地整理和消化原始资料，据此掌握系统所有期望的运行模式、状态和功能，主要步骤如下：

- ① 从任务要求和系统原理框图入手，对照功能描述文件，理解并标注系统功能，必要时，可根据理解重新画出系统原理框图。
- ② 检查详细电路设计，识别主要的功能部件。
- ③ 检查多张图纸通过连接器的电气连接。
- ④ 确定电源点、接地点以及重要的功能信号点。
- ⑤ 追踪并标注主要的功能信号从输入到输出的传播路径。



- ⑥ 根据功能信号的传播路径，重画系统功能信号流程图。
- ⑦ 标注可能的从输出到输入的反馈信号传播路径。
- ⑧ 标注电源供电和接地的网络。
- ⑨ 检查可能的绘图错误。

数据预处理的工作一般包括：为保证系统完整性而进行的系统补充定义、虚拟器件定义、连通性数据修补、系统划分、系统简化、建立元器件模型表、确定分布参数等。

其中，系统划分是指将复杂电路沿一定的界面，分割为简单的、易于分析的较小部分的过程，其原则是划分后的各部分电路之间不存在复杂的电气联系。根据这一原则，适宜作为划分的边界点为：电源供电点、各级别的供电母线（正母线）、各级别的供电返回母线（负母线）、电源返回点、集中接地点、指令信号总线、特殊功能节点、分系统边界等。

应确认电路沿边界点划分后不会导致忽略某些潜在状态。如果经划分后系统仍过于复杂，应进一步增加划分的边界点。

（2）分析阶段

首先是选定分析方法，选择基于拓扑模式识别或路径追踪分析方法的其中一种。若选择基于拓扑模式识别的方法，则可进行如下分析：

① 网络树生成。一般需借助计算机辅助分析软件工具进行。

② 拓扑模式识别。识别程序包括：从第一棵网络树开始分析；对每棵树，从系统的第一种运行模式开始分析；对每种运行模式（含不可忽视的过渡状态），首先由非断分支组成状态网络树，接着识别出网络树中所有可能的基本拓扑模式。

③ 结合线索表进行网络树分析。分析程序包括：对每棵树、每种运行模式中的各基本拓扑模式，结合开关状态表，回答线索表中的每个问题，借以发现潜在状态；重复上一步骤，直至完成所有的运行模式和网络树。

若选择基于路径追踪的分析方法，则步骤如下：

① 功能节点识别。识别程序包括：识别系统的运行模式和开关性器件的状态表；根据对系统的功能分析，完成目标的识别；根据对系统的功能分析，完成源的识别。

② 路径追踪。假定系统中所有开关性器件处于闭合位置，通过路径追踪，识别出在源和目标之间的所有路径。

③ 结合线索表的路径分析。分析程序包括：对每条路径，结合系统运行模式和开关性器件的状态表，识别路径的激发条件；必要时，追踪激发路径；对每个激

发条件进行分析,根据潜在分析线索表,识别出潜在状态;继续进行下一条路径的分析,直至完成对所有路径的分析。

(3) 结论阶段

结论阶段的程序如下:

① 记录分析结论,按潜在路径、潜在时序、潜在指示、潜在标志对问题进行分类汇总。

② 记录分析过程中发现的、可能的设计缺陷及资料错误。

③ 整理得到的结论,对发现的潜在问题进行分析,提出改正建议。

④ 将发现的问题提交设计方进行交流和确认。

⑤ 形成潜在分析报告。潜在分析报告的内容一般包括分析过程、分析结论、改正建议,以及与设计方交流和确认情况等。潜在分析报告的主要内容,也可用潜在分析报告简表的格式提供。

5.10 电路容差分析

5.10.1 容差分析的内涵

容差问题是电路输出的精度问题,另外,在一些关键电路部分,一些较大的电压波动会造成严重的器件失效,导致电路、系统故障。

电路性能参数发生变化的原因包括:

- 组成电路的元器件参数存在着公差。
- 环境条件的变化产生参数漂移。
- 退化效应。
- 元器件故障(不在容差分析考虑范畴)。

容差分析技术是一种预测电路性能参数稳定性的方法。它是研究电路组成部分的参数偏差,在规定的使用条件范围内,对电路性能容差的影响。容差电路的特点如图 5-35 所示。

容差分析的目的是分析电路的组成部分在规定的使用温度范围内其参数偏差和寄生参数对电路性能容差的影响,并根据分析结果提出相应的改进措施。

容差分析适用的对象以及开展时机如下:

- 适用于系统内的关键电路。
- 在设计早期初步电路原理图给出时开始。



- 在故障模式影响分析（FMEA）和降额设计之后进行。
- 在电路修改后进行。

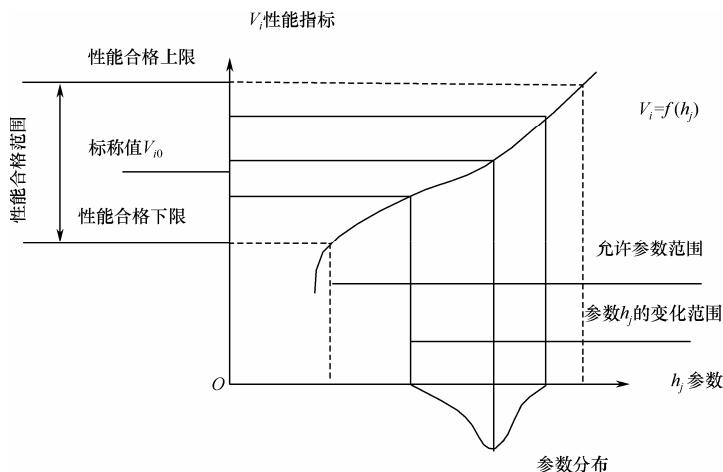


图 5-35 容差电路特点

5.10.2 容差分析程序

电路容差分析流程见图 5-36，主要步骤如下：

① 确定待分析电路，包括：

- 严重影响产品安全的电路。
- 严重影响任务完成的电路。
- 昂贵的电路。
- 采购或制作困难的电路。
- 需要特殊保护的电路。

② 明确电路设计的有关基线，包括：

- 被分析电路的功能和使用寿命。
- 电路性能参数及偏差要求。
- 电路使用的环境应力条件（或环境剖面）。
- 元器件参数的标称值、偏差值和分布。
- 电源、信号源的额定值和偏差值。
- 电路接口参数。

③ 对电路进行分析，得出在各种工作条件及工作方式下电路的性能参数、输

入量和元器件参数之间的关系。

④ 容差分析，包括：

- 适当选择一种具体分析方法。
- 求出电路输出性能参数的偏差范围，找出对电路性能影响敏感度较大的参数并进行控制，使电路满足要求。

⑤ 分析结果判别，偏差范围与电路性能指标要求相比较，比较结果分为两种情况：

- 符合要求，则分析结束。
- 若不符合要求，则需要修改设计，直到所求得电路性能参数的偏差范围完全满足电路性能指标要求为止。

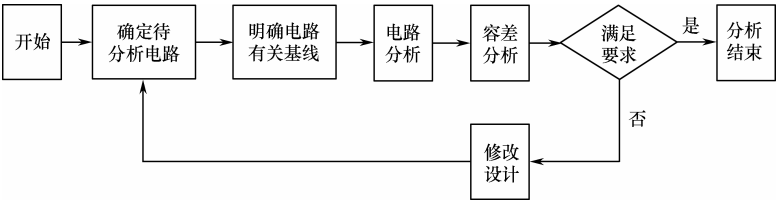


图 5-36 电路容差分析流程图

5.10.3 容差分析方法

容差分析的常用方法包括最坏情况试验法、最坏情况分析法、蒙特卡罗分析法、伴随网络法、阶矩法等，各种方法的特点见表 5-21。

表 5-21 容差分析方法汇总表

方法	电路模型	分析结果	优点	缺点	适用范围
最坏情况试验法	无	测试数据	不需要建立电路数学模型	必须在实际电路上才能进行试验	适用于可靠性要求高的电路
最坏情况分析法	要建立电路数学模型	电路性能参数偏差	简便、直观	分析结果偏于保守	线性展开法适用于分析精度要求较低的电路； 直接代入法适用于分析精度要求高的电路

(续表)

方法	电路模型	分析结果	优点	缺点	适用范围
蒙特卡罗分析法	要建立电路数学模型	电路性能参数的分布特性	最接近实际情况，能用 CAD	计算较复杂	适用于可靠性要求较高的电路
伴随网络法	支路的电流、电压方程，伴随网络的阻抗矩阵或导纳矩阵	电路输出参数偏差	能分析较复杂的电路，能用 CAD	计算复杂	适用于线性，时恒电路
阶矩法	要建立电路数学模型	电路输出参数均值、方差及容许偏差出现的概率	能反映实际情况，能用 CAD	计算较复杂	线性或非线性电路

5.10.4 容差分析实施要点

容差分析实施要点主要包括：

- 在设计早期给出初步电路原理图时就应该开始做电路容差分析。
- 电路容差分析工作应该以设计人员为主来完成，并在可靠性技术人员的配合下完成容差分析报告。
- 在应用最坏情况分析法时，要注意在设计参数变化范围内电路性能参数的变化趋势是否单调，如果不单调，则最坏情况分析会导致错误结果。
- 尽可能采用成熟的 EDA 软件实现自动化的容差分析，不仅可以提高分析的精度，而且可以降低复杂电路的分析难度。
- 为了简化手工计算的工作量，可以根据经验来确定容差分析必须考虑的重要设计参数，以缩小分析范围。
- 对于容差分析合格的电路，当设计改动时，应该再次进行容差分析。
- 对于容差分析不合格的电路，应该首先考虑缩小灵敏度最大的设计参数的偏差范围，然后再考虑缩小所有设计参数的偏差范围。
- 当采用缩小设计参数偏差范围的改进方法仍然不能满足要求时，应该考虑重新选择设计参数的标称值，使系统性能参数更稳定。如果没有更合理的设计参数以供选择，则应考虑修改电路的结构设计，采用更合理的电路结构来实现相同的功能。
- 对于容差分析合格的电路，当设计改动时，应该再次进行容差分析。
- 对于容差分析不合格的电路，应该首先考虑缩小灵敏度最大的设计参数的偏

差范围,然后再考虑缩小所有设计参数的偏差范围。

- 当采用缩小设计参数偏差范围的改进方法仍然不能满足要求时,应该考虑重新选择设计参数的标称值,使系统性能参数更稳定。如果没有更合理的设计参数以供选择,则应考虑修改电路的结构设计,采用更合理的电路结构来实现相同的功能。

5.10.5 使用软件工具进行容差分析示例

为了说明如何使用软件工具开展容差分析的过程,以电路故障仿真和最坏情况分析程序 CFSWCA (由工业和信息化部电子第五研究所开发) 为例,介绍使用 CFSWCA 进行容差及最坏情况分析的过程,界面如图 5-37 所示。

- ① 建立电路图:通过读取.net 和.cir 的电路文件建立电路图。
- ② 容差设定:通过添加、编辑模型参数来设定元器件模型的容差。
- ③ 容差注入:在电路参数列表中把故障模型注入电路中。

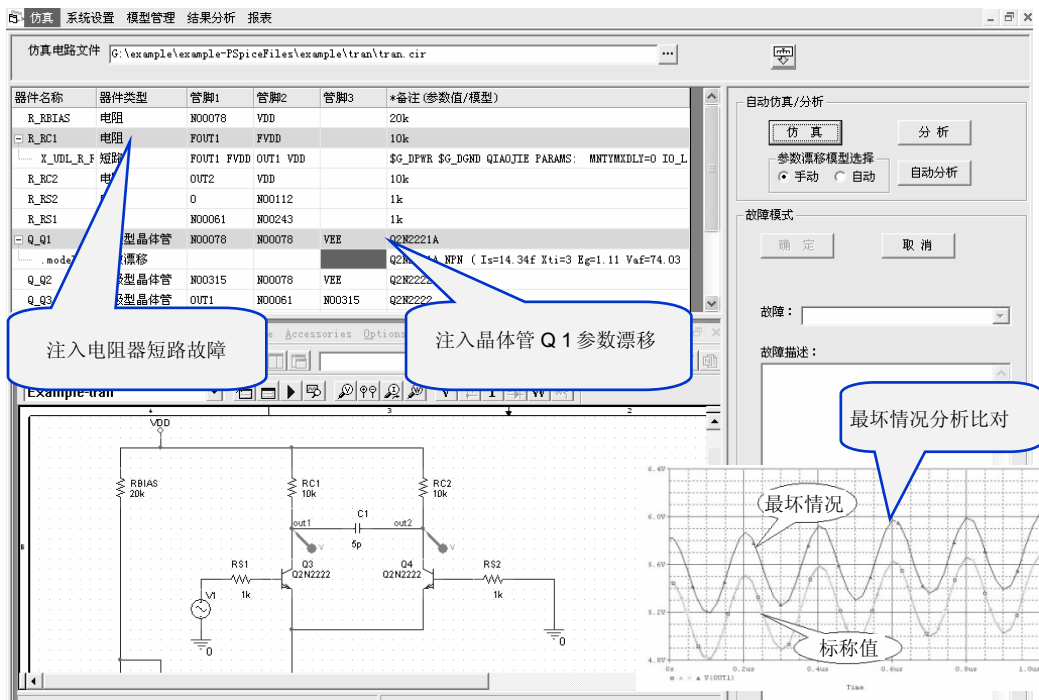


图 5-37 容差注入和最坏情况分析

- ④ 分析结果比较:单击“仿真”按钮,进行故障仿真和最坏情况分析,并进行结果比对。在图 5-37 中右下部的两条曲线分别是标称值情况和最坏情况的频响曲



线,通过对比分析正常与最坏情况下的电路性能输出情况,可辅助设计师进行电路的容差改进设计。

5.11 耐久性分析

5.11.1 目的

耐久性分析的目的是发现可能过早发生损耗的零部件,确定故障的根本原因和可能采取的纠正措施。

5.11.2 一般信息

耐久性分析传统上适用于机械产品,也可用于机电和电子产品。耐久性分析的重点是尽早识别和解决与过早出现耗损故障有关的设计问题。它通过分析产品的耗损特性还可以估算产品的寿命,确定产品在超过规定寿命后继续使用的可能性,为制订维修策略和产品改进计划提供有效的依据。耐久性通常用耗损故障前的时间来度量,而可靠性常用平均寿命和故障率来度量。

耐久性分析是用以确定产品在预期的寿命内能否保持足够的机械强度,根据分析过程获得的使用寿命估计值评价产品可靠性的方法,是识别呈现“早期”磨损失效的零部件和过程设计,隔离根本原因,从而确定可以采取的纠正措施。发现并解决这些设计问题,可为设计决策提供科学合理的依据,使产品更好地被市场所接受。耐久性可利用耗损出现前的时间来度量。

5.11.3 耐久性分析程序

估计产品寿命必须以所确定的产品耗损特性为依据。如果可能,最好的办法是进行寿命试验来评估,也可以通过使用中的耗损故障数据来评估。目前威布尔分析法是常用的一种寿命估算方法,它利用图解分析来确定产品故障概率(百分数)与工作时间、行驶里程和循环次数的关系。耐久性分析的原则:

- 应尽早对关键零部件或已知的耐久性问题进行耐久性分析。
- 应通过评价产品寿命的载荷与应力、产品结构、材料特性和失效机理等进行耐久性分析。
- 随着产品设计过程的推进,耐久性分析应迭代进行。

耐久性分析的程序如下：

- ① 确定工作与非工作寿命要求。
- ② 确定寿命剖面，包括温度、湿度、振动和其他环境因素，量化载荷和环境应力，确定运行比。
- ③ 识别材料特性，通常采用手册中的一般材料特性；若考虑采用特殊材料，则需进行专门试验。
- ④ 确定可能发生的故障部位。
- ⑤ 确定在所预期的时间（或周期）内是否发生故障。
- ⑥ 计算零部件或产品的寿命。

5.12 失效物理分析

5.12.1 概述

由于传统的基于数理统计的可靠性预计方法存在数据更新滞后、针对性差、统计模型有争议，以及预计结果不够准确等方面的问题，一种新型的基于失效机理、失效模式和失效应力的根本原因分析的可靠性评估技术被提出，这就是失效物理分析方法，该方法已经被证明对预防、检测和校正与产品设计、制造、运行相关的失效是非常有效的。实际上失效物理一词最早于 20 世纪 50 年代被提出，并于 1962 年举办了第一届失效物理研讨会，此后每年定期举办并延续至今，因此从严格意义上讲，失效物理分析方法其实并不那么“新”。

失效物理是由基本的机械、电子、热和化学过程决定的，通过了解可能发生的失效机理，可以发现新兴或现有技术中潜在的问题，并在问题发生前解决它们。若要确定失效机理，首先需要明确产品的温度、湿度、振动、冲击和其他可能的应力条件，接下来结合现有的有关所选物料和结构对应力的响应知识，进行应力分析，从而确定可能的失效位置、失效模式和失效机理，一旦明确了潜在失效机理，就可以使用特定的失效机理模型对产品进行可靠性评估，评估包括计算每种潜在失效机理的失效时间，然后选定最早发生的失效机理的失效时间来判断产品是否可以达到预期的使用寿命。还可以针对主要失效机理进行改进设计，增强产品耐用性，目前对于元器件级和板级失效物理分析，马里兰大学的 CALCE 电子产品与系统中心已经开发出了计算机软件，但其评估准确性还有待进一步验证。

失效物理方法研究的核心就是失效机理，按失效的发生特点，失效机理又可以分为耗损失效和过应力失效。耗损失效是指对器件或材料的损伤累积超过了其忍受极限而导致器件发生失效，耗损失效引起的设备失效可以通过可靠性预计预测其寿

命。过应力失效是指由于应力大于器件的强度，也就是说器件承受的应力在某一刻超过其忍受的极限而导致产品发生失效。另外，按照引起器件失效的应力类型，失效机理又可以细分为机械、电子、热、化学和辐射等类型，表 5-22 和表 5-23 给出了常见的失效物理分类信息，以及集成电路典型失效机理与失效模式。

表 5-22 常见失效机理类型

损耗型/过应力型	失效诱发应力类型	包含失效机理举例
损耗型	机械	疲劳、蠕变、磨损
	热	应力引起的扩散孔隙（SDDV）
	电	电子迁移、热电子注入、TDDb、表面电荷扩散
	辐射	辐射损伤、氧化物中电荷俘获
	化学	腐蚀、金属间生长
过应力型	机械	过弹性变形、屈服、断裂
	热	玻璃相变
	电	EOS、ESD、闩锁效应、绝缘层击穿
	辐射	单粒子偏转、单粒子烧毁
	化学	离子污染

表 5-23 集成电路常见失效机理与失效模式

器件类型	失效机理	失效模式	主要影响因素
集成电路	腐蚀	开路	温度、高电流密度、电过应力、沟道区大电场
	电迁移	开路、短路、高阻、漏电	
	时间相关的栅氧层击穿（TDDb）	阈值电压增大、开关电阻增大、效率降低	
	热载流子效应（HCI）	短路	
	负偏压温度不稳定性（NBTI）	参数漂移	
	单粒子效应（SEE）	状态翻转、烧毁	重力子辐射、原材料污染

5.12.2 失效物理模型示例

电子器件的失效物理模型描述了元器件失效的可靠性水平与可靠性相关因素之间的关联性，参照美国国家标准 ANSI/VITA 51.2 《失效物理可靠性预计》给出几种常见的失效物理模型示例。

1. 电迁移

电迁移是电场下导电电子与组成导体的金属原子之间发生动量交换，从而使金属原子发生移动的现象。电迁移的发生可能会造成局部的短路或断路，其失效时间与材料特性、电流密度、温度有关，由电迁移引发的失效率可用 Black 方程进行表征：

$$\lambda_{EM} = A_{EM} J^n \exp\left(\frac{-E_{aEM}}{KT}\right) \quad (5-43)$$

式中： A_{EM} ——与材料和工艺相关的常量；

J ——电流密度；

E_{aEM} ——特定温度下扩散对应的激活能；

K ——玻尔兹曼常数；

n ——对 Al 金属化而言，其取值与互连线中电流密度呈函数关系，比较近似的处理是：对宽线（平均晶粒度小于线宽）而言 $n=2$ ，对窄线（平均晶粒度大于线宽）而言 $n=1$ 。

激活能 E_{aEM} 与材料、特征尺寸（多大的金属空位或小丘可以引发失效）、晶粒大小和温度范围有关。表 5-24 给出了一些金属激活能的参考值。

表 5-24 金属激活能参考值

金属材料	晶粒尺寸 (μm)	E_{aEM} (eV)	n
Bulk Al	large	1.4	
Al	0.1~2	0.35~0.6	2~4
Al with 0.3%-5% Cu	1~6	0.5~0.8	2
Al-Cu-Si	0.25 ~ 0.6	0.25~0.86	1.7
Au	0.2 ~ 0.5	0.7~0.9	3.3~4

2. 热载流子注入

对 MOS 器件，热载流子是因为源、漏极电流流经沟道（漏极大电场）达到较高的能量，导致温度超出晶格温度而产生的，当载流子获得足够能量时，就可能越过金属-氧化物界面势垒注入栅氧化层中，导致电荷陷阱和界面态的产生，从而引起器件特性参数的漂移。热载流子注入失效可用幸运电子模型来描述：

$$\lambda_{HCI} = A_{HCI} \left(\frac{I_{sub}}{W}\right)^m \exp\left(\frac{-E_{aHCI}}{KT}\right) \quad (5-44)$$

式中： A_{HCI} ——特性相关因子；

I_{sub} ——峰值衬底电流（NMOS）、峰值栅电流（PMOS）；

W ——MOSFET 宽度；

m ——取值范围为 2~4；



E_{aHCl} ——激活能，取值范围为 $-0.2 \sim -0.1\text{eV}$ ；

K ——玻尔兹曼常数；

T ——温度。

3. 焊点热循环疲劳

热循环疲劳也叫低周疲劳，通常在温度波动比较大的情况下出现，可对焊点互连造成损伤，本质上是由于元器件与 PCB 板的热膨胀系数存在差异。在温度波动保持不变的情况下，热膨胀系数差异越大，在焊点处产生的应力也就越明显。焊点热循环疲劳失效时可用式（5-45）进行描述：

$$N_f = \frac{1}{2} \left(\frac{\Delta \gamma}{2\varepsilon_f} \right)^{1/c} \quad (5-45)$$

式中： N_f ——失效所需热循环次数；

$\Delta \gamma$ ——拐角焊点周期内剪切应力的变化幅度；

ε_f ——疲劳延性系数；

c ——疲劳延性指数。

对共晶焊料而言， $\varepsilon_f=0.325$ ，Engelmaier 给出：

$$c = -0.442 - 6 \times 10^{-4} T_{sj} + 1.74 \times 10^{-2} \ln \left(1 + \frac{360}{t_D} \right)$$

式中： T_{sj} ——循环周期内焊点平均温度 $=\frac{1}{4}(T_c + T_s + T_{C,O} + T_{S,O})$ ；

T_c , T_s ——芯片和衬底高温阶段的稳态温度；

$T_{C,O}$, $T_{S,O}$ ——芯片和衬底低温阶段的稳态温度，对非工作态，有 $T_{C,O}=T_{S,O}$ 。

对于共晶焊料（63/37,60/40）有引脚互联：

$$\Delta \gamma = \frac{F}{2(200\text{PSI or } 1.38\text{MPa}) Ah} \frac{K_D}{Ah} (\Delta \alpha L \Delta T_s - \Delta \alpha L \Delta T_c) \quad (5-46)$$

而对共晶焊料无引脚互联：

$$\Delta \gamma = \frac{F}{2h} (\Delta \alpha L \Delta T_s - \Delta \alpha L \Delta T_c) \quad (5-47)$$

式中： F ——经验修正因子；

h ——焊点表观高度；

K_D ——基于 Kotlowitz 方程的自由组件引脚的弯曲刚度；

200——63/37 和 60/40SnPb 焊料的剪切强度（PSI）；

1.38——63/37 和 60/40SnPb 焊料的剪切强度（MPa）；

$A = (2/3) \times$ 被焊引脚面积；

$\Delta\alpha$ ——组件与电路卡热膨胀系数之差；
 $L=(1/2)\times$ 引脚最大间距。

5.12.3 失效物理分析法应用示例

在失效物理分析方法的工程应用研究方面，美国马里兰大学开展得较为深入，其 CALCE 中心首先提出“基于失效物理的可靠性技术”概念及其技术框架，对基于失效物理的可靠性技术基础理论、建模和仿真分析方法、可靠性试验方法、产品可靠性评价方法、相关的基础材料数据库、失效物理模型及其参数数据库建设方面的研究都取得了长足进展，并开发了可靠性虚拟鉴定软件系统（CALCE 系列软件），已在 NASA 的航天飞船逃逸系统、HONEYWELL 公司的 AS 900 航空引擎电子控制系统等产品可靠性设计与评估中得到应用。目前国内部分机构，如工业和信息化部电子第五研究所、航空 301 所、北京航空航天大学等机构也对基于失效物理的可靠性分析与应用开展了研究，但工程应用成果尚不显著。工业和信息化部电子第五研究所近年来在失效物理方面开展的技术研究、试验技术、软件系统开发方面做了较多工作，设计开发了失效物理分析软件，并将该软件纳入到了工程软件 CARMES 中。

基于失效物理的可靠性分析方法主要可分为基础数据输入、建立环境剖面、应力仿真、基于失效物理实施可靠性评估几个步骤。

1. 基础数据输入

基础信息用以支撑各失效物理模型中除应力相关参数外其他参数值的确定，可分为板级、封装级和芯片级，表 5-25 和表 5-26 列举了可能涉及的基础数据类型。

表 5-25 板级基础信息类型

元器件信息	板级互连信息	裸板信息
✓ 器件类型	✓ 安装方式	✓ 印制板几何尺寸
✓ 封装形式	✓ 安装角度	✓ 印制板层数
✓ 封装几何尺寸	✓ 安装位置	✓ 印制板各层配比
✓ 封装材料	✓ 与板的相对高度	✓ 插入层几何尺寸
✓ 最大 I/O 数目	✓ 焊接方式	✓ 插入层材料
✓ 引脚几何尺寸	✓ 焊接材料	✓ 通孔数量
✓ 引脚中心距	✓ 焊接面积	✓ 通孔形状和几何尺寸
✓ 引脚材料	✓ 焊接材料高度	✓ 焊盘形状及几何尺寸
✓ 额定工作温度		✓ 印制板材料
✓ 结到壳的热阻		✓ 通孔材料
✓ 实际功耗		✓ 焊盘材料
✓		

表 5-26 封装级和芯片级基础信息

封装级信息	芯片级信息
✓ 裸片粘结材料	✓ 裸片几何尺寸
✓ 裸片粘结温度	✓ 裸片材料
✓ 裸片粘结层几何尺寸	✓ 氧化层厚度
✓ 引线框材料	✓ 氧化层材料
✓ 键合线直径	✓ 金属厚度
✓ 键合方法	✓ 金属宽度
✓ 密封材料	✓ 金属材料
✓ 密封温度	✓ 钝化层厚度
✓ 密封层几何尺寸	✓ 钝化层材料
✓ 引脚处理材料	✓ 最大电流密度
✓ 封装腔内水汽	✓ 最大工作电压
✓	✓

2. 建立环境剖面

环境剖面的建立需要完成两方面内容：一是采集产品的任务剖面信息，比如一架飞机在寿命期内会经历停靠与外出执勤两种状态，而外出执勤又可能包含诸如高原任务、空投任务等多种任务类型，每种任务可根据应力环境的变化进行更为细致的划分，如飞行前检查、准备起飞、外出飞行、降落、飞行后检查等阶段；二是确定环境剖面信息，即对不同任务阶段的可靠性相关应力状况进行定量描述，得到在产品任务阶段内各敏感应力量值水平及变化情况（通常以温度和振动应力最为常见），下面给出了某飞机电子控制器在高原任务下的温度与振动应力剖面，如图 5-38 和图 5-39 所示。

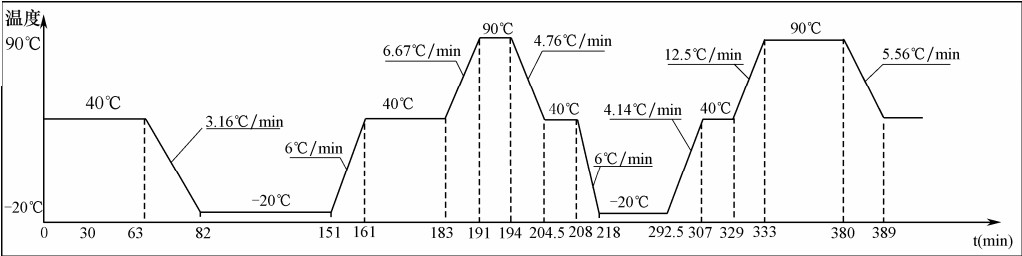


图 5-38 某飞机电子控制器在高原任务下的温度剖面

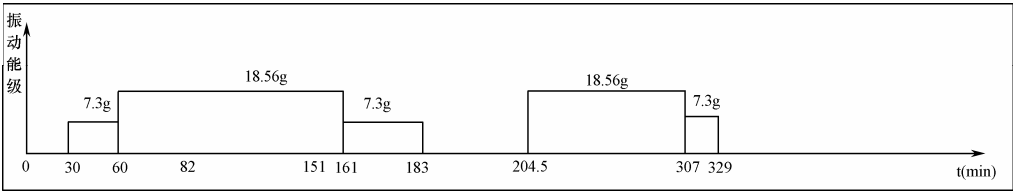


图 5-39 某飞机电子控制器在高原任务下的振动剖面

3. 应力仿真

完成上述工作之后，接下来需要结合环境剖面对产品进行应力仿真，得到产品对应力载荷的局部响应情况，用以明确失效物理模型中应力相关参数的取值。图 5-40 给出了飞机电子控制器在 40℃环境下的温度分布情况，图 5-41 给出了一定振动能级下的位移分布情况。

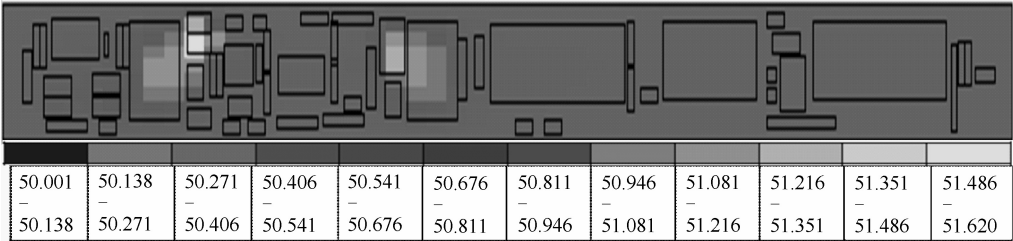


图 5-40 环境温度为 40℃时的温度分布

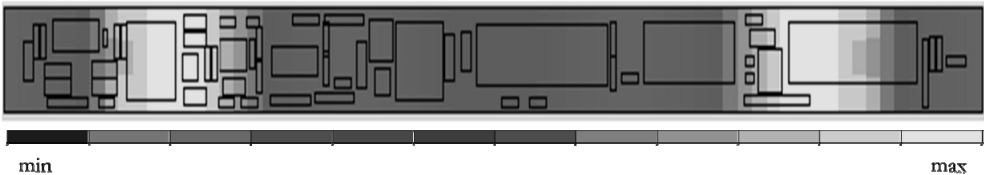


图 5-41 固有频率为 313.6Hz 时的位移分布

4. 基于失效物理实施可靠性评估

利用各失效物理模型和累积损伤理论，完成产品在特定任务剖面下的可靠性分析，得出产品的平均故障前时间和主要的失效机理。表 5-27 给出某飞机电子控制器的失效分析结果。

表 5-27 某飞机电子控制器的失效分析结果

元器件	累积损伤率	平均故障前时间 (年)	主要失效模式	主要失效机理	失效层次
TP7	~1.00	5.0	焊料开裂	焊锡热疲劳	板级
C18	~1.00	5.0	焊料开裂	焊锡热疲劳	板级
C5	0.75	6.60	焊料开裂	焊锡热疲劳	板级
C4	0.40	12.5	焊料开裂	焊锡热疲劳	板级
CR2	0.37	13.5	焊料开裂	焊锡热疲劳	板级
C10	0.20	25.0	焊料开裂	焊锡热疲劳	板级

(续表)

元器件	累积损伤率	平均故障前时间 (年)	主要失效模式	主要失效机理	失效层次
C2	0.18	27.7	引脚断裂	引脚机械疲劳	板级
R29	0.01	>30	裸片粘合剂开裂	粘结材料热疲劳	封装级
C9	~0.00	>30	键合线断裂	键合材料热疲劳	封装级
C19	~0.00	>30	裸片金属线开裂	电迁移	芯片级
...

完成失效物理分析之后，最短的平均故障前时间（本例中为 5 年）即可作为产品在该任务剖面下的寿命估计值，用以评估产品可靠性是否满足需求，并可在必要时结合失效机理（焊锡热疲劳）针对该薄弱环节实施定向改善，从而提升产品的可靠性保障水平。

基于失效物理的可靠性分析方法十分适用于查找与设计产品的薄弱环节，并定向改善，但在目前的工程应用、推广方面仍面临以下几方面问题：

- 操作较为复杂、成本高。
- 不适用于系统级的可靠性评估。
- 无法描述缺陷驱动的产品失效，在产品本身缺陷较多的情况下，其实际故障前时间可能会明显短于采用失效物理分析法得到的时间值。
- 失效物理模型的有效性有待进一步验证，同时由于国内外产品存在差异，目前在基本信息支撑方面较为薄弱。

5.13

机械可靠性

5.13.1

机械可靠性现状

由美国、英国、加拿大、澳大利亚和新西兰 5 国组成的技术合作计划（TTCP）委员会认识到需要联合起来发展一种新的机械设备可靠性预计方法。其目标是要根据机械设备单功能和多功能的设计特征、特定的使用环境，以及对载荷等因素的敏感性特点，编制出一本常用机械设备可靠性预计手册。手册中共计 4 组（18 种）设备和零部件，如阀门、调节器、作动器、汽缸、密封圈、弹簧、轴承等，都给出了具体的预计模型。他们还组织了专门的实验室试验及收集现场使用信息，以验证预计模型的正确性。

日本以民用产品为主，大力发展机械产品可靠性的应用研究。将 FMECA 技术成功引入到机械工业企业中。现在，日本一方面采用成功的经验设计，同时采用可靠性的概率设计方法结果以及与实物试验进行比较，总结经验，收集和积累机械可

可靠性数据。同时,日本还十分重视机械产品的可靠性试验、故障诊断、寿命预测、故障原因分析技术的研究和应用。

俄国对机械可靠性的研究十分重视,发布了一系列可靠性国家标准,这些标准主要以机械产品为对象,适用于机械制造和仪器仪表制造行业的产品,例如液压、润滑系统、发动机等。

在可靠性设计分析技术方面,目前国外研究较多的是结构可靠性和机构可靠性。结构可靠性主要是考虑机械结构的强度,以及由于载荷的影响使之疲劳、磨损、断裂等引起的失效。机构可靠性是指机构在规定的使用条件下,在规定的使用时间内,精确、及时、协调地完成规定机械动作(运动)的能力,用概率表示就是机构运动可靠度,包括典型结构运动可靠性、柔性机构动态强度可靠性分析。

目前结构可靠性的研究方法主要包括:

- 一次二阶矩法。
- 载荷和抗力安全系数法,使可靠性设计分析和可接受的设计方法联系起来。
- 响应面法。
- 均值法。
- 概率云图法。
- 响应面和蒙特卡罗综合法。

机构可靠性的研究方法目前主要是借助 CAD 软件,通过建立机械运动模型、运行仿真,统计机械产品的运行性能,可视化分析其可靠性水平。CAD 软件包括 ANSYS 公司的 FE-SAFE 软件、NASTRAN 公司的 ADAMS 等。

5.13.2 机械可靠性特点

机械产品可靠性与电子产品可靠性相比,具有许多不同的特点,了解分析这些特点,对于开展机械可靠性设计与分析具有重要意义。对主要特点综述如下:

- 电子产品的失效模式比较简单,而机械产品的失效模式比较复杂。
- 电子产品在使用过程中发生的故障主要是由于偶然因素造成的,而机械产品的故障原因主要是疲劳、老化、磨损、腐蚀等,因而主要是耗损型故障。
- 电子产品的应力易于预计,而机械产品的应力难于准确预计。
- 电子产品可以通过筛选等排除早期失效,在经济上是合理和有效的,而机械产品要开展这项工作在经济上通常是十分昂贵和困难的。
- 电子产品一般都是由标准的电子元器件组成的,而标准的电子元器件的基本失效率可看成常数。机械产品的功能零部件大多是非标准件,而且一种零部件常常要完成多种功能,使用环境又恶劣,因此,像电子产品一样统计其失效率是很困难的。目前已有的失效率统计模型及手册中的数据都不足以作为机械产品可靠性预计的直接依据。



- 电子产品推荐的维修主要是以更换元器件为主，而机械产品推荐的维修是修复和更换并重。
- 机械产品的寿命和可靠性试验一般是小子样的，而且，为了检测耗损型故障模式，所要求的试验时间较长，采用电子产品的可靠性鉴定试验统计方案往往是研制方无法接受和难以实现的，当然很多机械产品寿命分布不服从指数分布，因此，指数分布的统计试验方案也无法使用。
- 电子产品的可靠性数据已经形成了若干手册或文件，而机械产品的可靠性数据还十分缺乏。
- 机械产品可靠性要考虑载荷、几何尺寸、材料性能数据等因素的分散性和随机性。涉及很多学科，如力学、摩擦学、电化学等，这无疑给研究机械可靠性带来很大的困难。

5.13.3 结构可靠性分析

机械可靠性一般可分为结构可靠性和机构可靠性。结构可靠性主要考虑机械结构的强度以及由于载荷的影响使之疲劳、磨损、断裂等引起的失效；机构可靠性则主要考虑的不是强度问题引起的失效，而是考虑机构在动作过程中由于运动学问题而引起的故障。

结构可靠性是指结构在规定的时间内（设计使用年限）内，在规定的条件下（正常设计、正常施工、正常使用），完成预定功能的能力。结构的可靠性，包括结构的安全性、适用性和耐久性。结构失效可定义为“在规定的使用条件下，结构丧失其规定的功能”。一般也称为结构破坏。

疲劳寿命是影响结构可靠性的最重要因素之一。结构的全寿命可以分成裂纹形成寿命和裂纹扩展寿命。疲劳寿命一般指的是裂纹形成寿命。对于小尺寸构件，其裂纹扩展寿命很短，故常将其全寿命视作疲劳寿命。

大量试验结果和外场统计资料表明：结构或元件在名义上一致的条件下的疲劳寿命是一个分散性不可忽略的随机变量，而且其概率分布是偏态的。结构或元件的疲劳试验结果表明，结构疲劳寿命分布型式与电子元件寿命的分布型式不一致，不服从指数分布。在研究中，各国学者提出了多种型式的疲劳寿命概率分布。在工程上，目前应用最广泛的是两种：对数正态分布和威布尔分布。

到目前为止，广泛使用的疲劳寿命概率分布函数仍是对数正态分布和威布尔分布。在工程应用中，哪种分布更适用，可从以下几方面进行参考选择。

1. 对试验数据的拟合能力

在概率分布函数的中间区域，对数正态分布和威布尔分布两者通常都能得到较满意的结果。而在概率分布的两个尾部区域，要想通过试验来比较两种分布哪一个更符合实际情况是非常困难的，甚至是不可能的。

2. 疲劳破坏的物理模型

一般认为, 结构或元件的疲劳破坏应从最薄弱环节开始, 链式模型可能是合理的, 那么, 疲劳寿命分布就应为极小值分布, 而威布尔分布正是极小值渐近分布的一种形式。

另一种看法是, 结构或元件的疲劳寿命受到诸多随机因素的影响, 而且是众多因素的乘积效应在对疲劳寿命发挥作用, 因此, 用对数正态分布, 描述疲劳寿命的统计特性也可能是合理的。

对随机现象建立物理模型时, 总要提出若干假设, 这些假设是否正确, 归根到底还是要通过实践来证明。

3. 危险率函数的增减性

疲劳损伤累积过程是一种耗损破坏过程。根据人们长期的经验, 耗损破坏对应的危险率应该随使用时间的增长而单调地增加。对于威布尔分布, 当 $a > 1$ 时, 其危险率为单调增加函数。而对数正态分布的危险率则随使用时间的增加, 开始是上升, 最后却缓慢下降。

危险率随使用时间的进一步增加而下降, 这当然与耗损破坏的特性不相符, 但要注意, 对数正态分布的危险率在结构可靠性关心的低寿命阶段还是增函数。

4. 分布参数的数目

威布尔分布有三种参数形式, 对试验数据的拟合能力较强, 而且最小寿命参数比较符合实际情况。

5. 统计推断的简便性

在采用对数正态分布的前提下, 只要对寿命进行取对数的简单变换, 以后就可以利用基于正态分布的各种研究成果, 比较方便地进行假设检验、区间估计等对于结构可靠性分析、可靠性试验数据处理都十分重要的统计推断。而以威布尔分布为基础的统计推断则较困难。

5.13.4 机构可靠性分析

与结构可靠性相比, 机构可靠性的研究要晚些, 从 20 世纪 70 年代末期才开始研究, 到 80 年代才有了一些基础, 至 90 年代才有了一些成果。开展机构可靠性研究必须综合的运用机构运动学、机构动力学、机构精度学、摩擦磨损原理及可靠性工程等学科的最新成果。因此, 机构可靠性的研究是机构学研究的新领域, 也是可靠性工程在机械工程中应用的新方向。

机构磨损被认为是机构中最为突出的问题。在一般机械或飞机构造中, 机构运动副零件的磨损失效占总失效中相当大的比例。操纵机构、起落架收放机构、直升



机升力螺旋桨中的铰链接头与锁机构等都有因磨损失效而引起事故的实例。这些事故促使苏联的学者对机构磨损可靠性进行研究，由此在机构磨损的理论试验研究与使用统计方面都做出了杰出的贡献。

机构是指把机构通过运动副实现可动连接，并能够实现预期运动功能、承受并传递动力功能的构件。常见的机构形式：摇臂机构、连杆机构、齿轮机构、螺旋机构。机构的主要功能是实现预期运动、承受或传递动力。

机构功能可靠性是指机构在规定的条件下和规定的时间内，完成规定运动功能的能力。其中运动功能包括：

- 完成一定的运动形式，如飞机起落架收放机构执行收和放动作的功能。
- 在完成规定运动形式时，机构的运动参数保持在规定的范围内，包括机构运动位移、速度、加速度和时间等运动参数，如飞机起落架收放机构要求起落架在 10 秒内收起。

机构可靠性问题可简单地划分为承载能力可靠性（机械结构零部件可靠性）、运动功能可靠性（机构功能可靠性）。

影响机构可靠性的主要因素：

- 设计因素：包括机构的工作原理、动力源（电机等）、质量和转动惯量的随机特征。
- 生产因素：包括加工精度误差等。
- 环境因素：高（低）温、沙尘、腐蚀等。
- 使用因素：运动带来的磨损、动力源的恶化等。
- 人为因素：不及时维修、更换等。

5.14 元器件的选用控制

5.14.1 选用的必要性

电子元器件是高新技术武器装备的重要基础，其质量与可靠性直接关系到装备的技术性能、研制进程以及作战能力。因此，在装备设计过程中，最关键的一步就是做好元器件的选用控制，对于保障装备的性能和质量可靠性至关重要。

5.14.2 元器件选用管理的内容

作为装备用元器件选用管理的顶层标准，GJB 3404-1998《电子元器件选用管理要求》中给出了装备在研制、生产、使用各阶段，对电子元器件的选择、采购、监制、验收、筛选、保管、评审、使用、失效分析、信息管理等选用全过程的质量与

可靠性管理要求。在工程实践中,各武器装备或型号工程一般在 GJB 3404 的基础上,结合武器装备或型号工程的具体使用平台要求,制订各项元器件选用控制和管理工作的详细技术规范、要求或规定,以指导实际工作的开展。

依据 GJB 3404, 各装备承制单位一般按如图 5-42 所示开展相关工作。

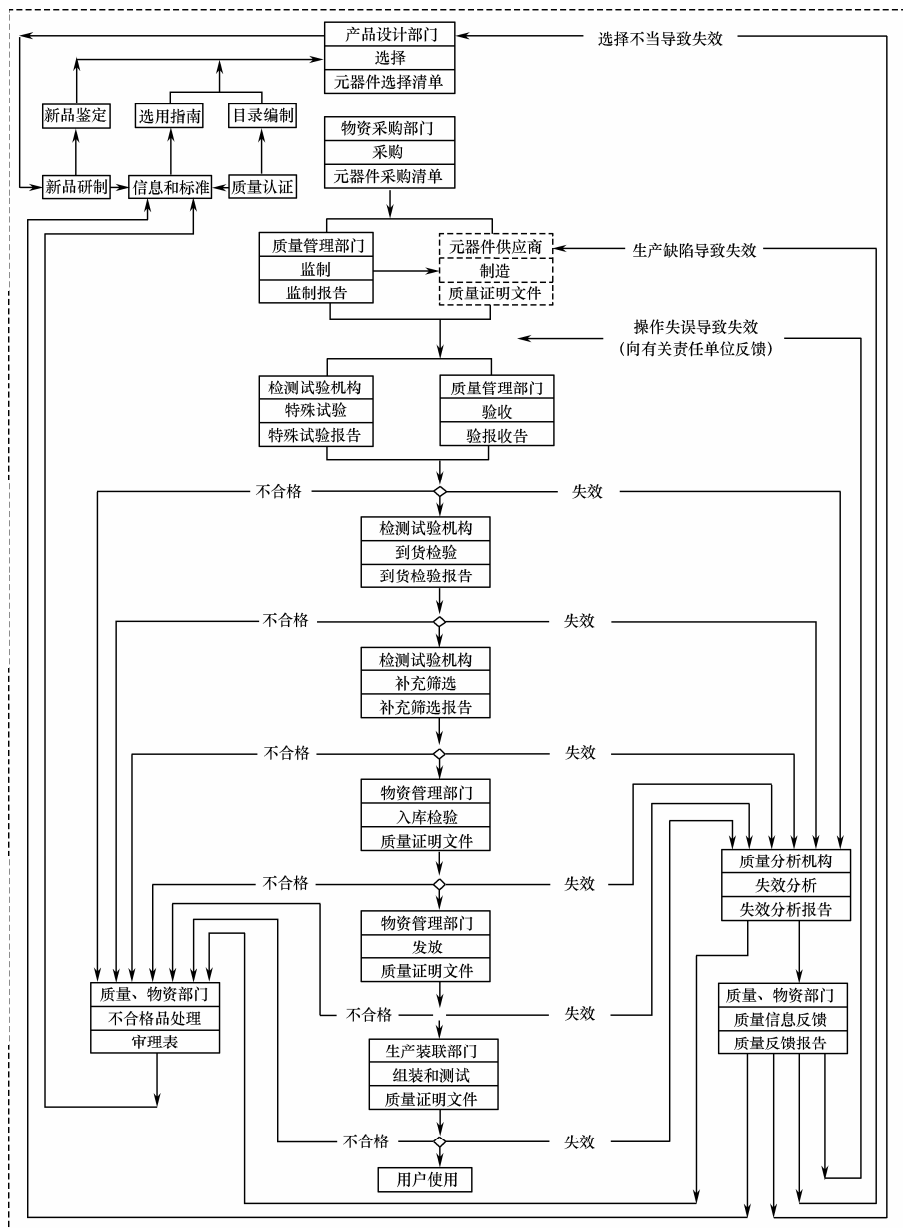


图 5-42 元器件选用和控制的工作流程图



上述 10 项工作涉及装备的产品设计、物资采购、质量管理、检测试验、生产装配、质量分析等多个部门。

具体要求如下。

1. 元器件选择

GJB 3404 规定：应制订装备用元器件优选目录作为设计选择、质量与可靠性管理、采购的依据。应严格按元器件优选目录选择元器件，超目录选择应严格审批。对元器件优选目录应实施动态管理，并应控制新研制元器件的选择，特别是用量小的（新研制的）专用元器件的选择。

选择是元器件管理工作的源头，选择是基础、是关键。它包括了型号根据各自的任務特点（如风险承受能力、成本、进度）对元器件适用性、常规可靠性、特殊指标的合理选择。

因而，开展元器件的选择时，应明确如下实施要点：

- ① 建立按照装备结构树的元器件基础信息库。
- ② 开展元器件清单审核或评审。
- ③ 编制《优选目录》，并动态更新，加强超目录管理。
- ④ 编制《禁用、限用元器件清单》。
- ⑤ 关键、重要元器件的选用控制。
- ⑥ 电子元器件停产断档管理。
- ⑦ 电子元器件统型优化实施。

2. 元器件采购

GJB 3404 规定：订购单位应编制采购文件，并按规定的程序履行审批手续，根据采购文件签订订购合同。

对于加强电子元器件的采购管理，应贯彻“保证质量、控制进度、节省经费、尽量集中”的原则，由采购部门统一协调、组织采购工作。

因而，开展元器件的采购时，应明确如下实施要点：

- ① 编制采购文件（含采购清单、采购规范和补充技术条件等），履行审批手续。
- ② 制订采购合同，在合同中应明确要求如下：元器件的名称、型号规格、数量、技术规范、质量等级、生产工艺、是否监制、验收方式、筛选与质量一致性要求、DPA 要求、生产和供货日期、防护要求、储存期、包装、运输、信息提供以及质量反馈等。
- ③ 电子元器件合格供方管理。
- ④ 加强进口电子元器件的采购管理，按正规渠道采购，确保质量，考虑国内是否具备复测及试验条件。

3. 元器件监制

GJB 3404 规定：凡在订购合同中规定了监制要求的元器件，应组织有监制资格的人员，按订购元器件批次，到元器件承制单位进行监制。监制应按规定的技术标准管理要求执行。

因而，开展元器件的监制时，应明确如下实施要点：

- ① 明确必须进行监制的元器件清单。
- ② 制订监制计划，编制监制与验收文件。
- ③ 组织有监制资格的人员实施监制与验收工作。
- ④ 对监制过程中出现的问题进行记录和协商解决。
- ⑤ 编制监制报告。

4. 元器件验收

GJB 3404 规定：验收应按规定的技术标准和管理要求执行。凡在订购合同中规定到承制单位验收的元器件，应组织有关验收资格的人员，按订购元器件批次，到承制单位进行验收。

因而，开展元器件的验收时，应明确如下实施要点：

- ① 明确必须进行验收的元器件清单。
- ② 制订验收计划，编制监制与验收文件。
- ③ 组织有验收资格的人员实施监制与验收工作。
- ④ 对验收过程中出现的问题进行记录和协商解决。
- ⑤ 编制验收报告。

5. 元器件筛选

GJB 3404 规定：对元器件应按有关技术标准的规定进行筛选，并提交筛选报告。对未经筛选的或经筛选但不满足要求的元器件，应做补充筛选或二次筛选，其筛选技术条件应按规定的技术标准执行。

因而，整机单位开展的元器件的二次筛选，应明确如下实施要点：

① 制定元器件二次筛选规范，明确各类别元器件筛选要求、筛选程序、方法和关键项目不合格率。

② 电子元器件在上机前原则上应 100% 的经过二次筛选，筛选批合格后方允许装机。

- ③ 应保留元器件二次筛选的试验记录。
- ④ 二次筛选合格的元器件应进行标记。
- ⑤ 筛选不合格的电子元器件不得装机使用。



⑥ 对在二次筛选过程中出现元器件失效应予以记录和失效原因分析。

⑦ 无条件进行二次筛选的电子元器件，在装配成部件、单元、设备、分机等时，必须进行环境应力筛选（ESS）。不符合 ESS 要求的电子元器件不能装机，符合 ESS 要求的电子元器件也要在各种试验中加强质量跟踪和控制。

⑧ 建立装机许可证制度。

6. 元器件保管

GJB 3404 规定：应制订有关元器件的与保管条件，包括存放、入库检查、定期检验、出库复查及元器件失效后的补发等要求，并贯彻执行。当元器件超过规定的有效储存期，应制订元器件超期敷衍要求，并按规定执行。

因而，整机单位开展的元器件的保管，应明确如下实施要点：

① 使用单位应建立完善、周密、严格的保管制度；保管人员应持证上岗。

② 储存与保管条件：元器件的储存与保管必须符合规定的储存保管条件，特别是对需要防潮、防腐、防锈、防老化、防静电等有要求的元器件更应妥善保管。

③ 存放要求：做到不同品种分类分批存放，库房内应标识明显、存放合理、排列有序、安全、整洁，温湿度应有记录。

④ 定期检验，在库房存放过程中应对有定期测试要求的元器件进行定期质量检验。发现不合格品时应及时做出标识、记录及隔离处理。

⑤ 超期复验。制订元器件超期复验规范，对超过储存期的元器件进行检验，检验合格后，经使用单位质量、标准化和主任设计师审批后方可装机。

7. 元器件评审

GJB 3404 规定：元器件评审应作为装备评审的一个重要组成部分。

根据电子设备研制的需要，按设备不同研制阶段，组织有关专家对选用元器件的质量与可靠性进行评审，并纳入电子设备的设计、工艺、质量评审中，评审内容可包括：

① 元器件选用是否符合优选目录的要求。

② 是否符合元器件规定的储存期的要求。

③ 是否按规定进行了验收、复验与二次筛选。

④ 是否按规定对元器件进行了 DPA，并对不合格批进行了有效的处理。

⑤ 是否按本规定对失效元器件进行了失效分析、信息反馈及采取了有效的纠正措施。

⑥ 选用《优选目录》外的元器件或更改选用的元器件时是否按规定办理了审批手续。

- ⑦ 元器件的使用（降额设计、热设计和安装工艺等）是否符合有关规定。
- ⑧ 元器件是否通过装机许可等。

8. 元器件使用

GJB 3404 规定：在合理选择元器件的前提下，还应采用降额设计、热设计、环境防护设计等可靠性设计技术，以提高元器件的使用可靠性。

因而，开展元器件使用时，应明确如下实施要点：

- ① 元器件装机前质量合格标记、证明文件以及性能检验。
- ② 降额设计。
- ③ 热设计及热测试。
- ④ 容差设计。
- ⑤ 耐机械应力设计。
- ⑥ EMC 设计。
- ⑦ 环境防护设施。
- ⑧ 可靠性预计。
- ⑨ FMECA。
- ⑩ 防静电设计。
- ⑪ 防潮湿、盐雾、霉菌设计。
- ⑫ 更改与代料等。

9. 元器件失效分析

GJB 3404 规定：应按有关规定，由指定的元器件失效分析机构进行失效分析。元器件失效分析后，负责分析的单位应按有关规定向委托单位提交失效分析报告，并及时反馈与上报有关单位。

因而，整机单位开展元器件的失效分析时，应明确如下实施要点：

- ① 发生关键、重要电子元器件失效，或多次、大量失效时，应按规定送授权实验室进行失效分析，查明失效机理，采取有效的纠正措施，防止重复失效的发生。必要时，应要求元器件生产单位及设备承制单位分别开展元器件质量归零和设计工艺归零。
- ② 对属批次性质量问题的，要及时发出元器件质量问题报警、通报。
- ③ 无论何时发现的失效（不合格）品应一律进行记录和隔离。
- ④ 元器件的失效分析报告应存档备案。

10. 元器件信息管理

GJB 3404 规定：应建立装备元器件的信息管理制度，指定有关部门收集、处

理、保管、定期发布元器件选用全过程的质量与可靠性信息。

因而，整机单位开展元器件的失效分析时，应明确实施要点：建立包含元器件选用、质量控制和使用等全寿命周期的质量与可靠性信息库，包括元器件选用基础信息库、元器件合格制造商信息库、元器件优选目录、进口电子元器件停产及替代信息库、元器件复验、筛选、DPA、失效分析等质量控制信息库、元器件装机使用可靠性信息库、元器件 FRACAS 系统等。

5.14.3 优选管理

选择是元器件管理工作的源头，它包括了电子设备根据各自的任务特点（如风险承受能力、成本、进度）对元器件适用性、常规可靠性、特殊指标的合理选择。不同的电子设备基于不同的任务要求和环境特点，对元器件选择的要求存在差异，因此，结合产品的具体使用环境特点，一般国产电子设备均会制订各项元器件优选的详细技术规范，以指导实际工作的开展。电子元器件选择的通用原则一般如下：

① 元器件的技术指标（包括功能性能、质量可靠性等）应满足装备使用要求，在选取过程中，应全面确认每个所选取的元器件，包括：

- 应明确所选元器件的使用环境条件（包括：温度、振动、冲击、湿度等），通过元器件数据手册和附加要求的元器件详细规范保证元器件能满足最终的应用要求。
- 对于货架元器件，至少应确认元器件生产厂的数据手册、元器件生产厂技术和应用说明、封装、可靠性和可获得性数据，以及可生产性数据（包括储存、焊接条件等）；对于定制的元器件，应确定特定的文件（包括说明书、生产厂数据和流程、可靠性、特定测试和筛选，以及相关的内部持续监控）。
- 元器件的可获得性和停产断档风险等级应作为元器件选择的一项重要判据。
- 对于有附加要求（如升级筛选、升额、附加参数定义等）的元器件，应作为与元器件不同的特殊元器件进行特别评价。

为确定元器件设计满足设备要求，应进行设计分析，包括：电磁兼容（EMC）分析、降额和应力分析、热分析、机械分析、测试、可测试性和维修性等。

② 元器件具有为装备配套的良好经历，未出现过因设计、制造、工艺等自身缺陷引起的重大质量问题。

③ 元器件的供方必须经过合格供方审核且列入《电子元器件合格供方名录》。一般对国产元器件供方的基本资质要求如下：

- 在中华人民共和国境内依法正式登记注册、具有法人地位。
- 具备从事元器件军工生产的相应资质，获得总装备部颁发的装备承制单位注

册证书或国防科技工业局颁发的武器装备科研生产许可证，且注册范围应涵盖元器件范畴。

- 通过 GJB 9001 质量体系认证，认证的产品范围应覆盖所提供的元器件类型。
- 应取得相应级别的保密资格认证，并制订相关保密措施，以确保相关外协方的保密工作符合规格要求。
- 具有为军工产配套元器件的良好经历，且产品质量可靠、供货稳定、价格合理，未发生影响航空装备质量的重大事故。

元器件供方在满足基本资质要求的基础上，还应满足以下条件：

- 国家持续资金投入。承担过总装军用电子元器件科研项目，亦或承担省部级、地方政府的电子元器件科研项目。
- 产品成熟且应用广泛。产品列入总装发布的《国产军用电子元器件产品手册》或型号工程的《电子元器件优选目录》。
- 元器件生产线稳定可控，包括：供方自身拥有已通过认证且正在维持的、有效的元器件贯标生产线；具有柔性生产、行业分工特点的部分类别集成电路，供方具有独立的设计能力，流片、封装、测试、可靠性试验等部分或全部环节外协且可控，对外包过程制订了详细的管理要求，实施了严格的质量控制，外包过程中的数据记录保持完整且可追溯。
- 元器件研制生产应符合相应国家军用标准，产品具有经过认可的军用详细技术规范。

④ 元器件的技术性能具有先进性；产品生产成熟、稳定，具有较长的产品生命周期；面临淘汰的元器件品种、规格以及按规定禁用材料、工艺、结构等不属于优选范畴。

⑤ 必须具有符合相应国家军用标准、经过认可的军用详细规范，产品必须通过第三方或双方组织的鉴定，包括：总装组织的产品（定型）鉴定、军厂双方组织的产品鉴定、随装备的设计定型或鉴定。

⑥ 元器件应是自主设计研发，原材料供应有保障，研制生产过程稳定可控，采用进口芯片封装的产品不属于优选范畴。

⑦ 元器件的供货稳定、有质量保证、产品性能和质量一致性较高，供货周期有保障、价格合理。

⑧ 元器件应具有军用级质量等级，产品出厂前应经过 100%筛选检验、产品持续进行质量一致性检验，具有质量考核和可靠性评价数据，记录完整，可追溯，应在 GJB/Z299 和 MIL-HDBK-217 最新版本中选取相应元器件的质量等级。

⑨ 元器件的工作温度范围，以及对振动、冲击、压力、潮湿和盐雾环境的耐

受能力应满足装备的使用环境条件要求，具有相应的见证数据。

⑩ 元器件应是标准化、具可推广性的元器件，定制型及非标准元器件不属于优选范畴。

⑪ 进口元器件尽量减少紫、橙、黄安全等级颜色的产品。

⑫ 关键、重要元器件、新研元器件以及寿命件的选用应特别注意。

对于可能危及人身安全、导致武器系统或完成所要求使命的主要系统失效，或如有故障，可能导致最终产品不能完成所要求使命的关键、重要元器件，如 CPU、FPGA、DSP、AD/DA 等完成系统主要功能的这类元器件应予以特别关注，要选用技术成熟、供货有保障的元器件，做好筛选、DPA、失效分析等质量控制工作，必要时可以下厂监制验收。

新研元器件主要是指刚研制成功，缺少工程应用验证的元器件，由于这类元器件缺乏工程应用经验，其随电路板、整机的潜在质量可靠性问题尚不可知，因此，新研元器件应进行充分的应用验证，包括元器件级、板级、设备级等应用验证，方可上机使用。

寿命件是指有使用循环次数（时间）限制，失效率随时间增长的耗损型元器件，如：示波管，这类器件应该在规定使用期终点加以更换，否则失效率将迅速上升。

此外，美军元器件的选择一般以美国国防机构批准使用的元器件管理标准 MIL-STD-3018《元器件管理》提出选择的基线原则，认为选用元器件时应重点考虑如下因素：

- 可利用性（非 DMSMS、成熟工艺、来源）。
- 应用情况（降额、元器件的使用、环境条件）。
- 成本效益分析。
- 元器件筛选。
- 鉴定试验数据或过往性能数据信息。
- 供应商选择。
- 元器件工艺/停产断档（查询 GIDEP 数据库或 DMSMS 库）。
- 与合同性能要求的符合性。
- 工艺匹配能力。
- 寿命周期成本优化。

5.14.4 质量控制

破坏性物理分析（DPA）、筛选、失效分析是电子元器件常用的质量控制手段。

1. DPA 分析

DPA 是通过微观物理手段确定产品质量的一种分析检验方法。主要目的是验证电子元器件的设计、结构、材料和工艺质量是否满足预定用途或有关规范的要求。由于某些项目必须解剖样品进行,因此分析检验的性质是破坏性的。

DPA 的试验依据是根据不同的元器件类型选择不同的试验项目和标准。与 DPA 试验有关的国内外标准如下:

① GB 2828-87: 逐批检查技术抽样程序及抽样表。该标准规定抽样产品的提交、样品的抽取、抽取方案、接收与不接收等。

② GB 4589.1-89: 半导体分立器件和集成电路总规范。

③ GJB 4027-2000: 军用电子元器件破坏性物理分析方法。该标准规定了电子元器件 DPA 的通用方法,包括 DPA 程序的一般要求、典型电子元器件 DPA 试验、分析的通用方法、缺陷判据。

④ MIL-STD-1580A: 电子、电磁和机电元器件破坏性物理分析。

⑤ MJL-STD-883: 微电子器件试验方法和程序。

⑥ GJB 548A-96: 微电子器件试验方法和程序。

该标准规定了微电子器件统一的试验方法、控制和程序,包括为确定对自然因素和条件的抗损坏能力而进行的基本环境试验;物理和电试验;设计、封装和材料的限制;标志的一般要求;工作质量和人员培训程序,以及为保证这些器件满足预定用途的质量与可靠性水平而必须采取的其他控制和限制,如:

- 方法 2009A: 外部目检。
- 方法 2010A: 内部目检(单片)。
- 方法 1018: 内部水汽含量。
- 方法 2012A: X 射线照相。
- 方法 2019A: 芯片剪切强度等。

⑦ GJB 360A-96: 电子及电气元件试验方法。

该标准规定电子电气的通用试验方法,主要试验包括环境类、物理性能类及基本电性能类属于 DPA 的项目:

- 方法 112: 密封试验。
- 方法 209: X 射线照相试验。
- 方法 217: 颗粒碰撞噪声控制。

⑧ GJB 128A-97: 半导体分立器件试验方法。

该标准规定半导体分立器件的通用试验方法,包括军用条件下抗损害能力的基本环境试验、机械性能试验和电特性试验,如:



- 方法 1018: 内部水汽含量。
- 方法 1071: 密封。
- 方法 207: 芯片粘附强度。
- 方法 2037: 键合强度。
- 方法 2076: X 射线照相检验等。

在上述标准中，GJB 4027 是开展 DPA 分析的主要依据。

2. 筛选

一般情况下，各类别电子元器件的寿命特性都可以用浴盆曲线来表示。

为了剔除早期失效的元器件，可采用质量和筛选试验。质量试验是通过检验或常规试验从生产线上剔除有缺陷产品的试验。筛选试验则是通过对批产品逐个施加一种或多种应力的方法剔除早期失效的元器件并降低失效率的试验。

元器件的筛选试验主要包括两部分：一部分是由制造厂对成品元器件进行的筛选试验，也称成品筛选；另一部分则是由使用方对承制方提交的对元器件进行的补充筛选试验。

(1) 成品筛选

成品筛选 100%由制造厂来进行，各类元器件大部分筛选项目相同，仅应力条件不同，这是因为各应力条件是由元器件自身特性、设计和工艺情况来确定的。

此外，各类元器件还有各自不同的筛选项目。相同筛选项目及效果如表 5-28 所示。

表 5-28 筛选项目及其效果对应说明

项 目	效 果	项 目	效 果
内部目检或镜检 (有要求时)	好	高温测试 (有要求时)	好
高温储存试验	较好	低温测试 (有要求时)	好
温度冲击试验	很好	密封试验 (密封元器件)	很好
颗粒碰撞噪声监测试验或 X 光检测	好	外观检测	好
老炼试验	极好	常温测试	好

(2) 补充筛选

补充筛选 100%由用户来进行，目的在于最大限度地剔除早期失效的元器件，补充筛选原则如下：

- 所进行的补充筛选应能有效剔除有关失效模式。
- 所进行的补充筛选应能明显降低装机后的失效率。
- 特殊筛选项目及超过一般正常筛选应力的筛选项目，其项目及应力的选择应

有充分的分析或试验依据，并保证对正常元器件不造成损坏、损伤，以及明显缩短其使用寿命。

补充筛选项目：

- 对元器件生产单位因某种原因未做或未按有关技术条件应力要求所做的筛选项目，可按有关技术条件应力要求补做有关筛选项目。
- 对元器件生产单位已按产品详细规范或有关技术条件的规定要求进行过筛选，但某些失效模式采取一次筛选难以有效剔除，而按原筛选要求重复进行筛选能收到较好的效果时，也应采取补充筛选项目。
- 原筛选项目提高筛选应力能收到较好的效果，在符合补充筛选的原则下，可提高应力补充筛选。

特殊筛选项目：采用针对某一失效模式的特殊筛选能收到有效的筛选效果时，应针对该元器件进行特殊项目筛选，但筛选项目的确定和应力选取应符合补充筛选的原则。

此外，对于进口元器件的补充筛选，可按高可靠规范采购，并有产地证明和质量保证文件时，一般可不再进行补充筛选。除此之外，均应进行补充筛选。

3. 失效分析

对电子元器件失效原因的诊断过程称为失效分析。进行失效分析往往需要进行电测量，并采用先进的物理、冶金及化学的分析手段。失效分析的目的是确定失效模式和失效机理，提出纠正措施，防止这种失效模式和失效机理的重复出现。

在电子元器件的研制阶段，失效分析可纠正设计和研制中的错误，缩短研制周期。在电子元器件的生产、测试和使用阶段，失效分析可找出电子元器件的失效原因和引起电子元器件失效的责任方。根据失效分析结果，元器件生产厂可改进元器件的设计和工艺，元器件使用方（整机厂）可改进电路板设计、改进元器件和整机的测试及使用的环境，或改变元器件的供货商。

由于失效样品数量极少，来之不易（往往经长期试验或使用后获得），内含重要信息，而失效分析过程大多具有破坏性和不可恢复性，为防止在失效分析过程中丢失证据或引入新的失效机理，失效分析应当按一定的程序进行。

失效分析的一般程序为：

- ① 收集失效现场数据。
- ② 电测并确定失效模式。
- ③ 非破坏性分析。
- ④ 开封装。



- ⑤ 镜检。
- ⑥ 通电激励芯片。
- ⑦ 失效定位。
- ⑧ 对失效部位进行物理分析和化学分析。
- ⑨ 综合分析，确定失效原因，提出纠正措施。

参 考 文 献

- [1] 张增照. 以可靠性为中心的质量设计、分析和控制. 北京: 电子工业出版社, 2010.
- [2] 曾天翔, 等. 可靠性及维修性工程手册. 北京: 国防工业出版社, 1994.
- [3] 康锐等. 型号可靠性维修性保障性技术规范. 第 2 册. 北京: 国防工业出版社, 2010.
- [4] 吴利荣, 王建华. 基本可靠性和任务可靠性模型研究. 现代制造工程, 2004.
- [5] GJB /Z 299C-2006. 电子设备可靠性预计手册.
- [6] 张文俊, 聂国健, 郑丽香. 国外最新可靠性预计方法综述. 电子产品可靠性与环境试验, 2009.
- [7] 张增照, 潘勇. 电子设备可靠性预计. 北京: 科学出版社, 2007.
- [8] IEC 61025: 2006 Fault tree analysis (FTA).
- [9] 孙红梅, 等. 关于故障树分析中几种典型重要度的研究. 电子产品可靠性与环境试验, 2007, 25 (2): 39~42.
- [10] 张大庆, 宋斌. 电子系统的潜通路分析技术. 光电技术应用, 43~46.
- [11] 李良巧. 机械可靠性设计与分析. 北京: 国防工业出版社, 1998.
- [12] 額田啓山. 机械可靠性与故障分析. 北京: 国防工业出版社, 2007.
- [13] 吴波, 丁毓峰, 黎明发. 机械系统可靠性维修性决策模型. 北京: 化学工业出版社, 2006.
- [14] 康锐, 石荣德. FMECA 技术及应用. 北京: 国防工业出版社, 2006.
- [15] QJ 3217-2005. 潜在分析方法和程序.
- [16] 任立明, 等. 潜在电路分析技术应用. 北京: 国防工业出版社, 2011.
- [17] GJB 3404. 电子元器件选用管理要求.
- [18] 孙青, 庄亦琪, 等. 电子元器件可靠性工程. 北京: 电子工业出版社, 2002.
- [19] 胡昌寿, 等. 航天可靠性设计手册. 北京: 机械工业出版社, 1999.
- [20] 王军生, 等. 导弹储存可靠性预测建模方法. 战术导弹技术, 2007.

第6章

可靠性试验与评价

6.1 概述

6.1.1 可靠性试验的目的

试验是产品研制和生产过程中改进产品设计、评价和考核产品的各项质量特性（如功能和性能、环境适应性、安全性、可靠性、维修性和测试性等）是否达到水平的必不可少的手段，已成为产品研制和生产工作的重要组成部分。可靠性试验是产品研制生产中要进行的关键试验之一，是产品研制和生产中可靠性工作的重要组成部分。

但是，人们往往把可靠性试验工作局限于在内场考核和评价产品的可靠性水平，因而重视可靠性鉴定和验收试验，忽视设计阶段前期的实验室可靠性研制和增长试验，以及投入使用后的使用可靠性评估和分析工作。从广义上说，凡是为了了解、评价、分析和提高产品可靠性水平而进行的试验，都称为可靠性试验。我们知道，只要有产品，就会有可靠性问题，它贯穿了从产品设计到产品寿命终了的整个过程。这个过程中，产品将经历设计阶段、生产阶段和使用维护阶段。在每个阶段，都可能出现各种各样的可靠性问题。可靠性试验实际上是一种获取产品在应力作用下有关信息的手段。这些信息有各种用途，随着获取信息目的的不同，可靠性试验的目的也不一样，主要包括下述几个方面。

1. 探索产品在各种应力条件下的可靠性特征

通过各种应力试验确定产品的寿命分布模型，给出产品各种可靠性特征量指标，如平均寿命、可靠寿命、故障率、可靠度等。如果已知产品的寿命分布模型，则通过可靠性试验以确定寿命分布中的未知参数，以及计算出各种可靠性特

征指标。

2. 发现产品设计、材料和工艺方面的缺陷

产品的可靠性是由设计引入的，因此提高产品可靠性的关键是充分利用各种可靠性设计和分析技术对产品进行精心设计。然而，即使是最好的设计师设计的产品也不可能没有缺陷，这些设计缺陷仅靠图纸检查、原理演示甚至仿真试验是不可能全部识别的。经验表明，大约有 70% 的设计缺陷主要通过对样件进行试验来发现，为改进设计提供了信息。产品设计完善的整个过程实际上是设计（再设计）与试验—分析—改进（即 TAAF 过程）的反复迭代。因此，可靠性研制试验通常被看成产品设计的组成部分，或者强化设计的一种有效手段。

3. 确认是否符合可靠性定量要求或评价产品的可靠性水平

可靠性鉴定试验是设计定型把关的手段之一。在产品的设计定型时，通过可靠性鉴定试验可以判断产品的设计是否符合规定的可靠性要求，防止可靠性设计较差、固有可靠性未达到合同规定的产品转入批生产。

在产品投入批生产以后，对批生产出厂的产品抽样进行可靠性验收试验，可以判断某批产品的可靠性水平是否达到了规定的指标，防止受制造和工艺水平影响，将可靠性达不到规定要求的产品交付给用户，保证交付产品的可靠性。

4. 为产品研制、使用和保障提供信息

如前所述，试验是获取产品信息的过程。各种可靠性试验，特别是可靠性研制试验，除了获取产品的故障信息以外，还可以对新材料、新工艺、新元件、新设计进行评价，暴露使用过程中可能出现的不安全因素，研究预防故障及危险发生的措施，获取产品对应力响应的特性、产品薄弱环节、产品功能、性能变化趋势等信息，这些信息使人们对产品有了更为全面的了解，可为产品的改进、使用和保障，以及评估产品的战备完好性、任务成功性、维修人力费用和保障资源费用提供信息，为进行有效的可靠性管理提供依据。

总之，通过可靠性试验可以确定产品在各种环境条件下工作或储存时的可靠性特征，为产品的设计、生产、使用提供有用的数据，并在试验中充分暴露产品在设计、原材料、工艺等方面存在的问题。通过失效分析、质量控制等一系列反馈措施，使存在的问题得以逐步解决，从而提高产品的可靠性水平。因此，可靠性试验是生产高可靠性产品的重要环节。

6.1.2 可靠性试验的分类及其主要用途

对于不同的产品，为了达到不同的目的，可以选择不同的可靠性试验方法。可

可靠性试验有多种分类方法，如以环境条件来划分，可分为模拟试验和现场试验；根据试验目的和用途可分为工程试验和统计试验；以试验项目划分，可分为环境试验、寿命试验、加速试验和各种特殊试验。下面给出几种分类方法，并简要说明各类可靠性试验的内涵和用途。

1. 一般分类

通常惯用的分类法，是归纳为环境试验、可靠性增长试验、可靠性增长摸底试验、筛选试验、可靠性测定试验、鉴定验收试验、寿命试验、现场统计试验、HALT/HASS 等，如图 6-1 所示。

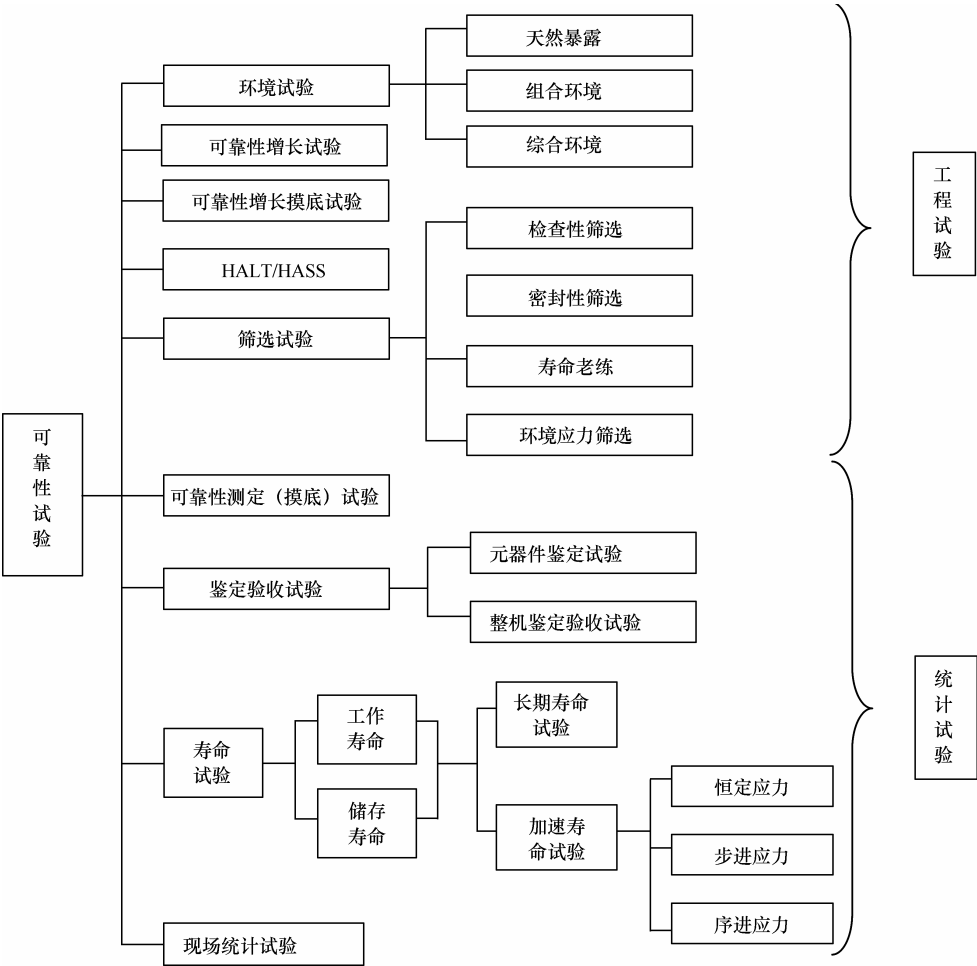


图 6-1 可靠性试验方法分类

表 6-1 列出了各种可靠性试验的原理、适用对象、应用时机、作用和特点。

表 6-1 可靠性试验简表

试验类型	试验原理	适用对象	应用时机	作用	特点
环境应力筛选 (GJB 1032)	工程经验	电子、机电产品; 器件、组件和设备	研制、生产和使用阶段	激发产品的设计和制造缺陷	100%进行,加速应力
高加速应力筛选 (HASS)	工程经验	电子、机电产品; 器件、组件和设备	研制、生产和使用阶段	激发产品的设计和制造缺陷	100%进行,加速应力
可靠性研制试验	工程经验	电子、机电产品	研制阶段	暴露产品缺陷	时间很长,无增长目标
可靠性增长摸底试验	工程经验	电子、机电产品; 设备级	研制阶段早期和中期	暴露产品缺陷	时间较短,约200h,无增长目标
可靠性增长试验 (GJB 1407)	工程模型	新研、关键重要的 电子、机电产品; 设备级	研制阶段后期	暴露产品缺陷	时间很长,有增长目标
可靠性仿真试验	故障物理学	电子产品; 模块级和设备级	研制阶段早期和中期	找出产品的薄弱环节	时间较短,加速应力或模拟应力
可靠性强化试验	故障物理学	电子产品; 模块级	研制阶段中期	找出产品的薄弱环节	时间较短,加速应力
基于故障物理的可靠性加速试验	故障物理学	电子产品; 设备级	研制阶段中期和后期	评估产品的可靠性水平	时间较短,加速应力
可靠性鉴定试验 (GJB 899A)	数理统计	电子和机电产品; 设备级和系统级	研制阶段后期 (定型阶段)	验证产品的可靠性水平	时间较长,模拟应力
可靠性验收试验 (GJB 899A)	数理统计	电子和机电产品; 设备级和系统级	批产阶段	验证批产产品的可靠性水平	时间较长,模拟应力

2. 可靠性统计试验和工程试验

根据试验的目的和用途，可靠性试验又分为统计试验和工程试验。

可靠性工程试验以保证和提高产品的可靠性为目的，为了达到这个目的，所采用的试验条件和方法，可以是多种多样的，特别是试验条件，它们完全可以不同于产品实际使用时遇到的环境条件。而试验方法越是能快速、高效地发现和暴露问题越好。试验的结果往往是希望能充分暴露产品存在的问题，以便采取有效的改进措施。

可靠性工程试验包括环境试验、可靠性增长试验、可靠性增长摸底试验、筛选试验、HALT/HASS 等。环境应力筛选是产品在研制生产过程中为了剔除材料制造

工艺的缺陷，排除产品的早期故障，使产品的可靠性得到保证的一种工序处理办法。而可靠性增长试验、HALT、环境试验则是通过试验来充分暴露产品的薄弱环节和激发产品的故障隐患，以进行设计、材料、工艺、结构或元器件等方面的改进，使产品的固有可靠性得以提高。

可靠性统计试验的目的是通过试验对产品达到的可靠性水平给出定量评估。可靠性统计试验包括产品研制开发阶段的可靠性测定试验（也称“摸底试验”）；设计或生产定型时的可靠性鉴定试验；批生产过程中产品交付时的可靠性验收试验、寿命试验、现场统计试验等。

可靠性测定试验是为了确定产品的可靠性特性，得出在规定条件下，可靠性状况的定量估计而进行的一种可靠性试验。其方法是利用试验过程中得到的产品故障信息，应用统计学的方法来推断产品达到的可靠性水平，最后导出描述产品可靠性状况的各种特征值。

可靠性鉴定试验是为了评价设计定型或生产定型的产品是否已经达到研制合同（或协议书）要求的可靠性指标而进行的一种可靠性试验。其方法是根据试验中产品发生的故障情况，得出可靠性是否合格的结论。另外，对那些在设计、工艺等方面有过重大变更的产品，一般也需要通过鉴定试验重新评价其可靠性水平。

可靠性验收试验是对准备交付的批量生产产品，验证其是否仍保持该产品鉴定时达到的可靠性水平而进行的一种试验。其采用的试验方法与可靠性鉴定试验一样，最终给出接收或拒收的判定。

可靠性测定试验、现场统计试验、可靠性鉴定试验和可靠性验收试验所给出的结论，都是统计意义上的结果，具有一定的置信度或概率特征，因此它们被统称为可靠性统计试验。

可靠性统计试验和可靠性工程试验的关系和区别如表 6-2 所示。

表 6-2 可靠性统计试验和可靠性工程试验对比表

试验项目	工程试验	统计试验
试验目的	保证和提高产品的可靠性	对产品达到的可靠性水平给出定量评估
试验条件	对暴露问题快速、有效	尽可能模拟实际使用情况
试验方法	多种多样不受限	需要满足一定的统计规则
试验结果	产品可靠性得到提高	产品可靠性得到评估

3. 可靠性加速试验与传统试验

为了适应日益激烈的竞争环境，企业必须在最短的时间内研制并生产出高可靠性的产品，以满足用户的需求。传统的可靠性试验方法已经不足以找出设计和生产

缺陷，或评估寿命预计值，于是人们纷纷把目光投向加速可靠性试验。加速可靠性试验通过采用比产品在正常使用中所经受的环境更为严酷的试验环境，在给定的试验时间内获得比在正常条件下更多的信息。因此，加速可靠性试验成为可靠性试验领域的重要研究方向。

可靠性加速试验也是一种统称。根据试验目的的不同，可靠性加速试验可分为加速寿命试验（ALT）、可靠性强化试验（RET）、高加速极限试验（HALT）、高加速应力筛选（HASS）和可靠性加速仿真试验等，如表 6-3 所示。

表 6-3 可靠性加速试验简表

加速试验方法	说明和用途
加速寿命试验 (ALT)	用加大应力的方法促使投试样品在短时期内失效，从而预测产品总体在正常储存条件或工作条件下的可靠性，确定产品在使用范围内的有效寿命。加速寿命试验按施加应力的方法大致可分为 3 种类型：恒定应力加速寿命试验；步进应力加速寿命试验、序进应力加速寿命试验
可靠性强化试验 (RET)	是一种步进应力试验，将小样本的产品暴露在一系列依次提高的某种应力（如温度或振动）台阶上，在每一应力台阶完成后，进行故障检测。这种试验被用来在一个比较短的时间周期内发现故障，也可用于确定产品在有效寿命期内抗随机故障的能力
高加速极限试验 (HALT)	是一种步进应力试验，经常将两种应力（如温度应力和振动应力）综合起来。这种高加速应力试验被用来尽可能快地发现故障，所用应力经常超出产品规定的极限
高加速应力筛选 (HASS)	这是一种筛选试验或用于生产的试验来清除早期故障，是一种积极的筛选，因为它实施的应力比普通的环境应力筛选（ESS）要高。当使用这种积极的筛选方法时，其所使用的应力水平应在可靠性强化试验或高加速寿命试验中确定
加速仿真试验 (AST)	通过基于故障物理的可靠性加速仿真试验，确定产品潜在故障位置、故障模式、故障机理等信息，准确定位薄弱环节及其主要影响机理，预测产品平均首次失效时间，利用加速试验模型确定加速试验方案

与传统的试验相比，由于可靠性加速试验使用了加大的应力条件，因此它可以加快产品内部物理变化及其影响的发生速率。这些现象包括结构变形（如弯曲或伸张）、化学反应（如腐蚀）或材料退化（如湿气渗透到一些合成材料内部造成的影响）。这些现象造成的物理变化最终会导致一种性能或结构方面可以检测到的不利变化，而通过采用加速试验，可以加快这些现象发生的速率，在试验室中用比现有方法更短的时间得到产品的有关信息，更快地获知产品的薄弱环节。因此可靠性加速试验是获得产品早期研制工作所需基本信息的一种非常有效的手段，可以通过选择一些特别的试验项目来识别那些以前知之甚少的潜在有害的产品特性，通过和不通过试验并不是试验的目的，而是获得更多的产品信息。

高加速应力筛选（HASS）旨在迅速地暴露产品的早期故障；可靠性强化试验（RET）则用以暴露与产品设计有关的早期故障，同时，也用于确定产品在有效寿命期内抗随机故障的健壮性；加速寿命试验（ALT）的目的是找出产品是如何发生、何时发生和为何发生耗损故障的；而基于故障物理的可靠性加速仿真试验的目的则是基于故障物理的可靠性建模仿真，确定产品潜在故障位置、故障模式、故障机理等信息，并根据仿真应力和加速模型预测产品平均首次失效时间。

可靠性加速试验与传统的可靠性试验相比，在试验目的、性质、应力等方面都有很大差别。表 6-4 将两类试验技术进行了简要的对比分析。

表 6-4 可靠性加速试验与传统可靠性试验对比表

对比项	可靠性加速试验	传统可靠性试验
试验目的	迅速暴露产品潜在缺陷，保证产品具有要求的可靠性水平	观测产品的可靠性水平，保证用户接收到合格的产品
试验属性	是一种激发试验，不存在试验是否通过的判决条件	是一种模拟试验，具有试验是否通过的判决条件
环境应力	使用加大的环境应力，不考虑产品使用的某种条件	模拟产品在实际使用中的典型环境
试验方案确定依据	根据产品故障机理和故障物理分析结果确定	根据统计原理确定
所用应力确定依据	根据产品设计的极限应力和产品的工作极限应力条件确定	根据产品实际使用条件确定

4. 按试验截尾情况分类

根据试验截止情况分类，可靠性试验可分为：

- 全数试验：样本全部失效才停止试验。这种试验可以获得较完整的数据，统计分析结果也较为可信，但是所需试验时间较长，甚至难以实现。
- 定时截尾试验：试验到规定的时间，不管样本失效多少，试验即截止。
- 定数截尾试验：试验到规定的失效数，试验即截止。若规定失效数为全部试样 n ，即为全数试验。

根据试验中失效发生时是否用新样品替换后继续试验，又分为有替换和无替换两种，于是，可靠性试验可有以下组合：

- 有替换定时截尾试验。
- 有替换定数截尾试验。
- 无替换定时截尾试验。



- 无替换定数截尾试验（包括全数寿命试验）。

6.1.3 可靠性试验的要素

1. 试验样品

根据试验性质的不同，用于可靠性试验的样品，其来源及技术状况将有所不同。从统计学角度讲，用于试验的样品应能代表总体的特征，因此试验样品一般要求从总体中随机抽样得来。应该说，那些经过精雕细刻、特殊加工“开小灶”后的“工艺品”是不符合统计试验要求的，它们缺乏代表性。显然用这样的样品来进行试验，所得到的试验结果仅代表试样本身的特征。然而，除了可靠性验收试验是在产品批量生产时进行的，可靠性测定试验和可靠性鉴定试验，特别是设计定型时进行产品可靠性试验一般都不具备较大的批量，因此严格地规定试验样品的技术状态，是使试验结果具有代表性的重要保证。一般来说，试验结果只代表与试样具有同设计、同材料、同工艺的产品的可靠性状况，尤其对研制产品而言，其技术状态的变动较大，专门加工、精心制造在所难免，因此在试验时对其技术状态的冻结与确认是十分必要的。这样就能使试验结果具有明确的阶段性与代表性。

为了使试验具有一定的广泛性与经济性，可靠性统计试验的样品数目，在保证每台（套）样品有足够的试验时间长度的前提下以多为好，一般要求不要少于 2 台（套）。

2. 试验条件

可靠性试验的条件既要考虑到受试产品的固有特性，又要考虑到影响受试产品故障出现的其他因素。一般来说，可靠性试验所指的规定条件通常需要根据产品实际使用的环境条件确定。对于大多数产品来讲，其实际使用环境是十分复杂的，因此可靠性试验如选择在现场进行，当然是一种最真实的使用环境，但是这种环境是多变的、不可控制的，随时都会遭受各种自然因素的影响。因此在确定试验条件时，要注意受试环境的代表性。只有在具有代表性的试验条件下得到的产品可靠性的评价才会更符合产品的真实使用情况。

确定产品试验条件的一般方法是：根据产品的使用过程（或称任务剖面），找出与其对应的环境条件（或称环境剖面），然后再将其转化成适合于工程模拟的试验条件（或称试验剖面）。

我们把产品投入使用后执行各种使命的过程称为任务剖面，一系列不同的使命过程就构成了不同的任务剖面。而对应于不同的任务剖面（如室内、室外、白天、夜晚、热带、寒带、陆地、海上、高空、地面、机载、车载、工作、储存等），产

品所经受的环境条件也是大不相同的（如温度、湿度、气压、振动等），这就对可靠性试验条件的选择提出了要求。

在现场进行可靠性统计试验时，应选择能代表产品使用过程中可能遇到的各种任务情况，那些受地域、季节或一些不可控突发因素等影响，只能反映某些任务状况的试验条件是不可取的。

在实验室进行可靠性统计试验，其所用的试验剖面应该是产品完成各种不同任务剖面时所对应的各种不同环境剖面的综合。GJB 899A-2009 中的附录 B 较详细地介绍了由任务剖面确定试验剖面的步骤及其综合方法。作为试验剖面应给出描述试验条件的具体环境参数，以及其施加方式和程序，如温度变化范围及其变化速率；湿度或气压变化要求；振动方式及其量级；多环境因素综合施加还是逐项或单项施加等。

产品在使用过程中可能遇到的因素是多种多样的，也是复杂多变的，要想在实验室里进行完全复制式的模拟是不可能的，也是不必要的。实验室可靠性试验通常选用产品使用过程中经常遇到的，对其可靠性有较大影响的环境因素来进行模拟，如高低温、湿度及振动等。另外，从工程实现的复杂性、可能性及经费等方面考虑，产品在使用过程中可能遇到的某些特定或极端环境，如盐雾、高湿、沙尘、冲击、雨淋、日照、辐射、气压等，通常作为环境试验项目进行专项考核。

为了能有效地模拟真实的使用环境，目前多因素综合环境应力试验已在可靠性试验中得到广泛的应用与推广。由于受环境试验设备制造技术的限制，早年的实验室可靠性试验，其环境应力的施加，都采用单项独立方式进行，或是将单项按时序组合的方式进行（见图 6-2），这与产品实际使用遇到的环境相差甚远，特别是有些只有在综合环境条件下（即二项或多项环境应力同时施加），才能发生的产品故障机理将得不到激发，如低温条件下加振动，对脆性材料或热胀冷缩材料的影响，与单一低温再加常温的振动对它们的影响是完全不同的，这将造成试验结果与实际使用（多环境因素综合）情况差距较大，此种情况在试验中已被多次证明。近年来，随着认识的深入和试验设备制造技术的不断改进，将几种环境应力条件综合在同一试验过程中已成为可能。中国赛宝实验室（CEPREI），从 20 世纪 80 年代中期起已率先在国内对电子设备开展了温度、湿度和随机振动等综合环境应力的可靠性增长与鉴定试验，取得了很好的效果（见图 6-3）。在此示范效应下，目前国内已广泛采用综合环境应力进行各种可靠性试验。国军标 GJB 899A 和 GB 5080 提供了多种设备的综合环境试验条件，可供使用参考。

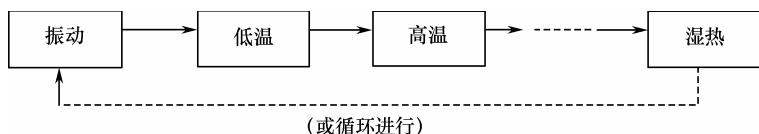


图 6-2 组合环境应力试验示意

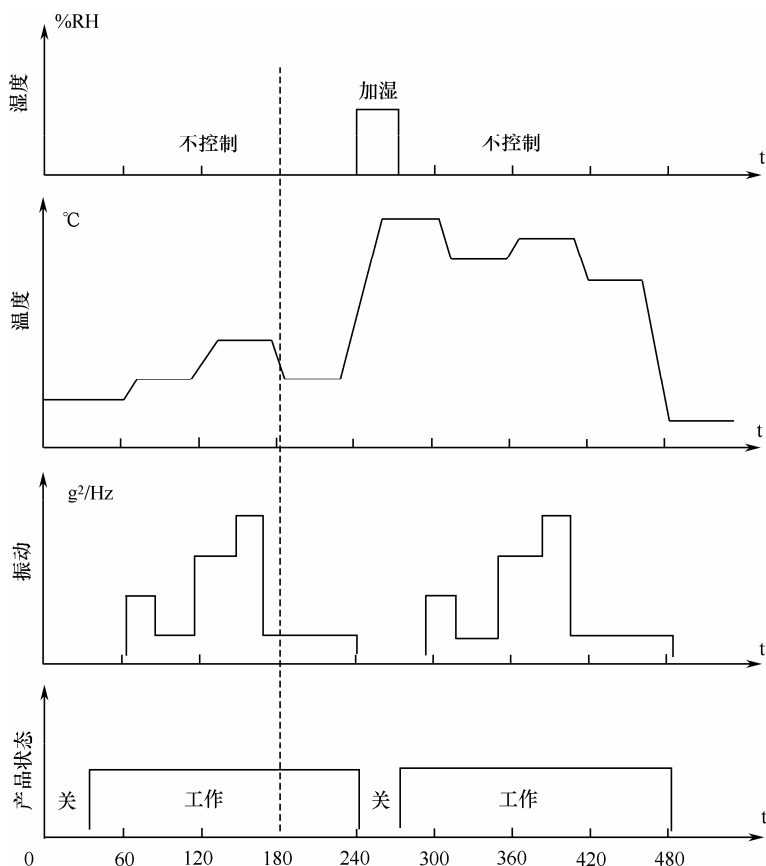


图 6-3 组合环境应力试验示意

3. 试验时间

试验时间是受试样品能否保证持续完成规定功能期限的一种度量。广义的时间包括工作次数、工作用期和距离等，对不同类型的样品要求的试验时间也不相同。

4. 故障判据

确定故障判据对可靠性试验数据的准确采集以及试验实施都是关键性的工作，确定故障判据的原则如下：

① 试验样品在规定的工作条件下运行时，任何机械、电子器件、零部件的破裂、破坏，以及使样品丧失规定功能或参数超出所要求的性能指标范围，都作为故障计入。

② 由于试验设备、测试仪器或工作条件的人为改变而引起的故障，不应计入为故障。

5. 可靠性试验数据的收集与处理

(1) 可靠性数据收集

可靠性数据是产品的可靠性预计、设计和试验的基本条件，是提高产品可靠性的根据，所以对数据的收集、积累、交换、分析和处理是可靠性工作的中心任务之一。可靠性数据可以来自现场试验或模拟试验，包括系统、设备、模块、元器件、零部件和原材料的数据都需要收集、分析和处理，以便为进一步开展可靠性设计分析和试验评价打好基础。在收集数据时必须注意以下几点。

- ① 收集对象和范围要明确和统一，否则容易发生差错。
- ② 注意对试验结果进行去伪存真的分析处理，确保数据的有效性。
- ③ 要保证原始数据的真实。影响因素有：抽样方法、试验的环境设计（如工作条件和试验应力的选择）、统计设计（如样本容量、测试周期、试验停止时间、抽样方案等的选择），以及试验设备和测试仪器的精度等。
- ④ 要保证原始数据具有足够的信息量。只有在原始数据达到一定的信息量以后，才能使产品的寿命分布及其可靠性特征的结论准确可靠。
- ⑤ 要选择合理的统计分析方法。

(2) 可靠性试验数据的记录

产品可靠性试验中的数据记录，可采用表 6-5 的形式。

表 6-5 可靠性试验数据汇总表

生产厂名			产品名称		型号 规格	
产品生产日期			试验条件		可靠性指标	
试验日期	自 年 月 日 时到 年 月 日 时		试验标准、方 案等编号			
故障发生时间	故障现象和 原因	失效件型 号和规格	失效件的出厂 日期和生产厂	替换和维 修	故障判据（包括主要性能指标）	
累计试验时 间（小时）			预计值		置信水平	
生产厂名			产品名称		型号 规格	
累计失效数			点估计值		估计值下限	
累计修理时 间（小时）					估计值上限	
停机时间 （小时）			数据员 （签名）		试验结论	

填表人（签名）

填表单位（盖章）

填表日期：



(3) 可靠性试验数据的分析

分析试验数据的目的是要得出能判断预先预想的目标（或模型）与所得到的结果是否相符的结论。分析的方法是统计学的数值分析法（或图分析法），以及对试样的物理、化学、结构、材料强度的失效物理分析法。

(4) 可靠性试验数据的处理

因为试验观测结果具有一定的随机性，一般原始数据都具有集中性和分散性的特征。为了反映这些数据的统计特征，常用统计量来表示，对数据的集中性常用算术平均值、几何平均值、中位数等统计量来表示，对数据的分散性常用极差、方差或标准方差等统计量表示。数据处理的方法很多，常用如下一些方法。

① 利用频数（或频率）或相对频数的数据，绘制直方图，获得失效时间分布密度和其他可靠性特征量。

② 利用图分析法和最小二乘法。

③ 利用数据统计分析法。

本书的第7章将专门讨论可靠性数据的收集与分析处理问题，这里不再赘述。

6.1.4 可靠性试验的计划与要求

1. 可靠性试验计划

为了节省试验时间和费用，保证试验结果正确可靠，在试验开始前，在充分研究、分析的基础上，制订详细的可靠性试验计划。试验计划应当提出试验的目的、要求、条件、程序，以及试验过程中必须注意的细节或说明。其详细程度应能保证试验人员顺利操作，并处理试验过程中可能遇到的问题。可靠性试验计划（有的国家也称可靠性试验大纲）一般应包括如下内容：

① 产品的可靠性要求。

② 可靠性试验目的及条件。

③ 可靠性试验的进度计划及费用预算。

④ 可靠性试验的方案。

⑤ 受试产品的要求（包括受试样品数量及说明、受试设备检测安排及要求等）。

⑥ 可靠性试验中对产品性能的监测要求。

⑦ 可靠性试验用的设备、仪表。

⑧ 试验结果的数据处理方法。

⑨ 试验报告的内容。

⑩ 时间和试验人员。

2. 可靠性试验要求

对产品可靠性试验的要求一般是指在产品合同或产品标准中,在拟定试验方案时应考虑到的要求。

(1) 受试产品及试验种类

可靠性试验适用于研制的模型或样机、批量生产的任何产品,但总体(是指所要研究的对象的全体,这里的全体是指产品的某一技术参数)必须在本质上是统一的,即产品是以相同的方法、在同样条件下生产的。受试产品必须从所代表的总体中随机抽取,如果需要的话,还要规定抽样程序。

实施试验的类型可以是实验室试验或现场试验。

(2) 可靠性特征及统计试验方案

选择拟采用的分布类型、适用的可靠性特征或分布参数以及统计试验方案。对于可靠性验证试验,产品在实际使用条件下的可靠性要求(指标)总是被转换为验证试验的要求。当可靠性特征是指一个系统的可靠性特征并且是由分别验证的各单元的可靠性特征推导出来时,则应规定所采用的包括可靠性方框图的推导程序。

(3) 试验条件和试验周期

① 工作及环境试验条件。

应尽可能包括实际现场使用中主要的工作和环境条件,包括产品的功能模式、输入信号、设备的实际操作(要求)、能源(电、水、压缩空气),以及电负载、机械负载、功率输出等负载条件。

现场使用的环境条件通常是由不同严酷度的许多环境因素组合和顺序构成的。对实验室来说可以单独地、组合地或顺序地施加环境因素。

GB 5080.2-86 给出了选定工作条件和环境条件的详细导则。

② 试验期间的预防性维护。

典型的预防性维护种类是功能检查、更换、调整、校准、润滑、清洗、复位、恢复等。

预防性维护原则上应与实际使用所进行的维护一致。

③ 上述①和②两项组合及顺序即为试验周期。

(4) 受试产品的性能监测与失效判别

应规定试验过程中需要监测的受试产品的功能参数(主要是输出参数),以及相应的测量方法、测量精度、估计总测量误差的程序。在不能连续地进行监测的情况下,则必须确定监测间隔,以及在试验周期中应进行监测的测量点。

应规定每个要监测参数的可接受的极限范围,以便失效判别。在产品试验标准中一般应给出典型的失效类别,以供参考,包括需要立即做出拒收判决的失效类别和应计入产品非关联失效的失效类别。还应规定每一个产品相应的、最小和(或)

最大的相关试验时间。

(5) 试验前的准备和故障检修

在可靠性试验前，应对受试产品进行测试、调整、校准及老练。受试产品的任何老练或其他预处理应力（例如装卸或运输）应与可交付使用的所代表的总体产品所承受的应力相等。

采用的故障检修程序，即在试验期间允许修复或更换的等级（单元、部件或组件、零件或元件等）。

3. 可靠性试验大纲

统计试验的进行必须按照可靠性试验大纲所规定的试验计划来执行，试验大纲要对可靠性试验提出各项规定与要求。由于可靠性试验大纲是开展各项试验活动的依据，因此，编制试验大纲是试验前首先要做的一项工作。试验大纲一般应包括如下要素。

(1) 试验目的与要求

大纲首先必须说明本次试验要达到的目的及其试验性质：是可靠性测定试验、鉴定试验或验收试验。要对试样的构成做出限定，对评估或考核的可靠性指标做出明确要求。

(2) 试验条件与方法

大纲要按照产品的研制合同或任务书、产品技术条件或相关技术条件的要求，对样品的受试环境条件和试验方法做出规定。

(3) 试样状态与来源

大纲要对投试样品的技术状态及其来源做出具体规定，如说明是哪个阶段的研制样机、或是定型样机、批生产样机；是抽样还是送样等等。

(4) 试验组织与管理

可靠性试验涉及的部门和人员较多，为使试验能有序、有效地开展，大纲必须明确试验的组织机构与管理方法，以协调工作，实施试验和条件保证，进行故障处理与信息反馈，以及完成样品性能监测与试验监控等工作。

作为可靠性鉴定试验，按 GJB 899A 和 GB 5080 要求，必须成立由产品研制方、使用方和试验方三方组成的联合试验小组来具体负责处理试验过程中发生的各种问题，包括：试验的中止、试验的继续、故障的确认与处理，以及试验前、试验中及试验后的评审等工作。

(5) 试验进度与地点

大纲要求对试验的地点加以明确，并对试验的进度做出要求，以控制试验的时

间与经费。

(6) 试验评审与报告

为保证试验有效地进行,大纲可对试验进程中的关键时刻提出进行评审的要求,如试验开始前对试样、参试仪器、设备、人员及条件保证等的准备状况进行检查与确认,即开展试验前评审;试验中样品故障或设备故障修复后,全新投入试验时进行状态的再确认,即试验中评审;试验结束时对试验情况进行汇总,对试验结论达成共识,即试验后评审。评审一般可由联合试验小组自行进行,大型、复杂或关键系统的试验可邀请专家共同进行评审。

大纲还必须明确试验报告的内容与要求,以及负责报告编写的部门与人员,鉴定试验报告将根据联合试验小组提供的各项试验记录与评审意见,一般由试验方负责编写。

(7) 试验结束后故障与样品的处理意见

为了尽量避免和预防试验中发生的故障模式在生产和使用中再次发生,大纲可对试验后故障的处置提出要求;也可以结合实际情况对受试样品提出处理意见,以达到物尽其用,节约人力、物力与财力的目的。

6.1.5 可靠性试验方案及一般程序

1. 产品可靠性试验方案

应依据试验大纲所规定的试验目的、试验要求、试验条件和试验方法等内容来制订具体的、详细的试验实施方案。

试验方案主要包括:

- ① 试验项目。
- ② 试样构成与数量。
- ③ 统计试验方案选择。
- ④ 确定试验环境条件及其施加方式。
- ⑤ 试样性能测试项目与时间。
- ⑥ 故障判据。
- ⑦ 试验设备及配套测试仪器。

统计试验方案和试验环境应力条件的确定是试验方案的核心。由于统计试验方案的选择涉及试验要达到的目的、可靠性指标的评价要求,以及要投入的时间和样品数量等重要问题,因此,在制订方案时必须认真对待,方案的选择必须要权衡各方面的因素,以及人力、物力和财力的许可。根据试验性质的不同,可选择不同的

统计试验方案，如定时截尾试验、定数截尾试验、序贯截尾试验、可提前接收的定时截尾试验、成功率试验，以及全数试验等。使用时可参见 GB 5080 和 GJB 899A 等有关标准。一个必须引起注意的问题是：统计试验方案一旦确定，在试验中就不得随意更改，这是因为试验方案的中途更改会引起统计模型的变更，其结果计算方法也大不相同，由此引起的试验结论也会发生本质的变化，因此在试验方案中必须详细叙述所选定的统计试验方案的内容，以及对试验结果数据处理方法的约定，以便试验结论具有准确性、唯一性与可比性。

由于可靠性指标是对产品在规定条件下完成规定功能能力的一种定量描述，即使对同一个产品，其经受的环境应力条件不同，将产生的可靠性试验结果也不同，因此试验方案应根据试验大纲规定的试验环境应力条件，制订实施方案，并确定各应力条件的大小，如温度变化范围、温度变化速率、高温限、低温限、各温度时间、加湿时间及量值、振动谱形及量值（正弦定频、正弦扫频、宽带随机、正弦+宽带随机等）。另外，还要明确各应力条件的施加方式及程序，是用单项应力环境，还是将几项环境应力组合起来逐次施加（即组合环境），或是将它们综合起来按一定的方式同时施加（即综合环境）。

在试验方案中必须事先给定试验样品的性能测试或功能监测的具体时间点。可靠性试验与环境适应性试验的差别在于：在整个试验过程中，环境适应性试验一般不要求试样工作，其性能测试仅在试验结束后才进行，看其有无变异，因此对某些自行恢复的故障与缺陷，在环境适应性试验中是无法及时发现的。而可靠性试验要求样品按照考核的需要设定状态，产品在大部分时间都要求处于工作状态，因此需要对其试验过程进行性能或功能的监测，以及捕捉和发现样品发生的问题；试验中对样品性能的监测时间点设定就显得十分重要。一般的原则和经验是把监测点定在环境应力条件较严酷的时候，如样品经受最高或最低温度时、高潮湿度时、振动量级最大时等情况下进行样品性能或功能的监测。其目的是考察样品在恶劣环境下能否保持良好的性能。那种在试验中随意设定或任意进行样品性能测试的做法是不可取的。

在试验方案中还必须明确地给定对故障的判据，这也是获得统计试验结果的依据。没有合理、准确的故障判据，就不可能得到合理、准确的统计试验结果，也不能得到对产品可靠性的准确评价。另外，对试验中发生的各类故障还必须按其性质不同对它们进行必要的故障分类：如关联故障、非关联故障、责任故障与非责任故障等。关联故障一般是指产品在试验中所发生的故障，在实际使用条件下也会发生的故障。当出现关联故障时还需要进一步分清是属于责任故障还是非责任故障。所谓责任故障是指出现的故障是由产品本身的问题引起的故障。在进行可靠性试验结果的统计处理时，只计算责任故障的次数。有关故障分类的详细信息，可参见 GJB 451A-2005 等标准。

2. 产品可靠性试验的一般试验程序

可靠性试验的一般试验程序如图 6-4 所示。

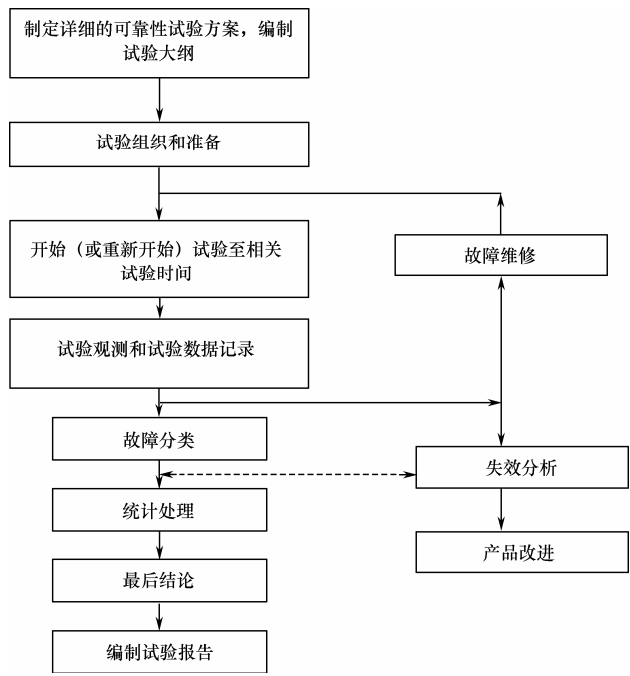


图 6-4 可靠性试验的一般程序

试验中应给每一个受试产品建立一份试验记录，并按先后顺序在规定的的时间和每次失效之后进行数据记录，最好是连续记录试验条件和受试产品的性能。每个受试产品的记录应包括下列内容：

- ① 观测到受试产品的任何失效、其他有关事件、采取某项措施的日期和时间，以及经过的相关试验时间。
- ② 失效分析的详细情况，以及已知的有关失效分类的所有重要资料，包括参照的失效报告。
- ③ 任何事件或措施，包括详细的可靠性试验方案中规定的预防性维护项目的说明。
- ④ 更换或重新安装单元、零件（元件）等的识别标记。
- ⑤ 工作条件和环境试验条件。
- ⑥ 验证故障检修有效性的时间。
- ⑦ 试验人员和受试设备（产品）操作人员的姓名。

试验记录和失效分析报告是可靠性试验的全部原始资料，是开展可靠性工作的

基础，应妥善加以保管，最好运用信息管理系统加以管理。

6.2 可靠性测定试验和可靠性增长测定试验

6.2.1 可靠性测定试验

可靠性测定试验通常是在产品完成研制的初期，希望摸清所研产品当前达到的可靠性水平和存在的问题时采用的一种试验方法，因此也有人将其称为“可靠性摸底试验”。

产品可靠性指标的测定不同于对产品其他性能指标（如技术参数）的测定，因为所谓产品的可靠性指标，实质是要给出产品发生故障的定量描述，而产品故障的发生是一种随机事件，需要较长时间，积累一定数据后才能发现它的这种统计规律，因此产品可靠性指标的测定试验一般都采用较长时间的寿命考核方法进行。

1. 试验简述

根据产品的特点与试验目的的不同，测定试验有在产品工作状态下进行的，也有在储存状态下进行的。常见的可靠性测定试验方法是在模拟环境条件下对产品进行寿命考核。由于试验条件是采用模拟环境条件，与真实环境有差异，因此在确定环境条件时，应注意选择具有代表性的试验条件，以使得到的产品可靠性评价更接近实际使用情况。关于“试验条件”和“试验样品”的选择和确定，可按照前面章节叙述过的有关原则进行。

在进行产品的可靠性测定试验时，一般采用截尾试验的方法，有定时截尾与定数截尾试验之分。所谓定时截尾，就是当试验进行到预定的试验时间 T 时试验就终止，然后根据试验中产品发生的故障个数，对产品的可靠性做出评估；所谓定数截尾，就是当试验进行到预定的故障个数 r 时试验就终止，然后根据试验终止时所累积的总有效试验时间，对产品的可靠性做出评价。可见这两种试验方法，都是在部分产品出现故障时就停止试验，这样我们就可在相对短的试验时间内得出试验的结果，那么从统计学角度考虑这种截尾试验方法得到的试验结果是否会误差大一些呢？可以证明：试验结果误差的大小，不是截尾试验方法造成的，而是由统计学参数决定的。因为从统计学的角度分析，既使我们等到所有投试样品出问题，那也未必能说该试验结果就百分之百精确。因此我们在实际试验操作时，不必要也不可能等到所有试样全部出现故障时，才对其进行可靠性评估。而采用截尾试验方法，尤其是定数截尾试验是目前最常用的方法，具有很强的计划性和可操作性。

为了及时发现和记录受试样品出现的故障，在进行可靠性测定试验时，必须对

产品的技术性能进行监测。理想的做法是在试验时，试样的各项技术性能通过自动测试设备进行监测，以便及时发现试样发生的问题，为试验评估提供准确的信息。但实际上目前大多数产品不具备这种条件，因此在进行可靠性测定试验时，一般采用定时测量的办法，即在预先商定好的时间点上对试样进行性能监测。当发现问题时，为统计故障产品的有效试验时间，可以取前次测试点与当前测试点的平均时间，也有干脆只算至前次（未发生故障时）测试点的时间。具体做法，可视试验情况事先约定。

在进行可靠性测定试验时，另一项必须在事先要做的工作是约定试验中判别产品故障的标准，即制订“失效判据”。一个产品性能的好坏，通常是由许多技术指标来进行判断的。在可靠性试验中除有特殊说明外，一般的做法是：只要有任何一项不合格，就计为产品不合格。而引起产品（特别是电子设备）不合格的原因，可能是由某一个，但也可能是由某几个元器件或工艺的问题引起的。当确认这些失效/故障是独立发生，而不是从属发生（即由一个发生，引起另一个也发生）时，则凡是独立的都应计为一次故障。换句话说，即在可靠性试验中不是简单地统计产品的不合格数，而是要统计发生独立故障的个数，这是值得注意的一个问题。

2. 参数估计

对于寿命服从指数分布或近似服从指数分布的产品的 MTBF 可按下列办法进行点估计和置信限估计。

(1) 点估计

测定试验 MTBF（平均故障间隔时间）点估计值如下：

$$\theta = \frac{T}{r} \quad (6-1)$$

式中， r 为试验中产品发生的责任故障总数； T 为所有参试样品有效受试时间的总和，即：

$$T_{r,n} = \begin{cases} \sum_{i=1}^r t_i + (n-r)t_r & (n, r, \text{无}) \\ \sum_{i=1}^r t_i + (n-r)t_0 & (n, t_0, \text{无}) \\ nt_0 & (n, t_0, \text{有}) \\ nt_r & (n, r, \text{有}) \end{cases}$$

式中， n 是投入试验的样品数； t_0 是定时结尾试验的结尾时间（h）； t_r 是定数截尾试验中出现 r 个故障的时间（h）； t_i 是第 i 个受试样品的故障时间（h）； $(n, t_0, \text{有})$ 表示有替换定时截尾试验； $(n, r, \text{有})$ 表示有替换定数截尾试验； $(n, t_0, \text{无})$ 表示无替换定时截尾试验； $(n, r, \text{无})$ 表示无替换定数截尾试验（包括全数寿命试验）。

**【例 6-1】计算点估计值**

有 3 台设备，每台进行了 200 小时的试验，试验中失效 6 个，有替换，计算其平均寿命的点估计值。

MTBF 点估计值： $\theta = (200 \times 3) / 6 = 100\text{h}$ 。

(2) 单测置信限

测定试验的 MTBF 单测置信下限估计值：

$$\theta_L = \frac{2T}{\chi^2_{2r+2, \alpha}} \quad (6-2)$$

式中： θ_L ——规定置信度水平下的 MTBF 的置信下限；

T ——试验总时间；

α ——显著性水平， $(1-\alpha)$ 为置信度；

$\chi^2_{2r+2, \alpha}$ ——自由度为 $(2r+2, \alpha)$ 的 χ^2 分布。

测定试验的失效率单测置信上限估计值：

$$\lambda_U = \frac{\chi^2_{2r+2, \alpha}}{2T} \quad (6-3)$$

在实际使用中，一些 χ^2 分布的数值可由 Excel 的 CHIINV 函数计算获得。

【例 6-2】计算置信度下限值

有 3 台设备，每台进行了 200 小时的试验，试验中失效 6 个，有替换，计算其平均寿命的 90% 置信度下限值。

MTBF 90% 置信度下限为：

$$\begin{aligned} \theta_L &= \frac{2 \times 3 \times 200}{\chi^2_{14, 0.1}} \\ &= \frac{1200}{21.06} = 56.97 \end{aligned}$$

3. 双侧区间估计

测定试验 MTBF 双侧区间估计为：

$$\theta_L = \frac{2T}{\chi^2_{2r+2, \alpha/2}} \quad \theta_U = \frac{2T}{\chi^2_{2r, 1-\alpha/2}} \quad (6-4)$$

测定试验失效率双侧区间估计为：

$$\lambda_L = \frac{\chi^2_{2r, 1-\alpha/2}}{2T} \quad \lambda_U = \frac{\chi^2_{2r+2, \alpha/2}}{2T} \quad (6-5)$$

【例 6-3】点估计与区间估计

对 20 个电阻器进行 120℃ 的高温试验，其中失效 12 个，失效时刻分别为：

270、420、500、920、1380、1510、1650、1760、2100、2320、2350、2650 (h)。

假定该电阻器的失效服从指数分布, 试求其 120°C 的平均寿命 θ 的点估计及区间估计值 (置信度 $1-\alpha=80\%$)。

$$\text{解: } T = \sum_{i=1}^{12} t_i = (n-r)t_s = 17832 + 8 \times 3000 = 41830$$

$$\theta = \frac{T}{r} = \frac{41830}{12} = 3486$$

按区间估计公式其下限值 θ_L :

$$\theta_L = \frac{2T}{\chi_{2r+2, \alpha/2}^2} = \frac{2 \times 41830}{\chi_{26, 0.1}^2} = \frac{2 \times 41830}{35.56} = 2352.64$$

θ_U 为:

$$\theta_U = \frac{2T}{\chi_{2r, 1-\alpha/2}^2} = \frac{2 \times 41830}{15.66} = 5342.27$$

用 Excel 计算时, 调用函数 CHIINV 计算 χ^2 的区间点, $\text{CHIINV}(1.0, 26) = 35.56$; $\text{CHIINV}(0.9, 24) = 15.66$ 。

【例 6-4】试验时间的推算

服从指数分布的某电台, 其产品说明书上要求 MTBF 达到 3000 小时, 现从中随机抽取 5 台进行寿命试验。在不发生一次故障的条件下, 最少试验多少小时才算合格 (取置信度 90%) ?

解: 由平均寿命的下限估计式可知:

$$\theta_L = \frac{2T}{\chi_{2r+2, 1-\alpha}^2}$$

有:

$$\begin{aligned} \theta_L \cdot \chi_{2r+2, 1-\alpha}^2 &= 2T \\ \therefore T &= \frac{\theta_L \cdot \chi_{2r+2, 1-\alpha}^2}{2} = \frac{3000 \cdot \chi_{2, 0.9}^2}{2} = \frac{3000 \times 4.606}{2} = 6915.00(h) \end{aligned}$$

因此, 需要有 7000 小时的总试验时间, 如果以 5 台进行试验, 则需要试验 $7000/5=1400$ 小时, 也就是说, 需要取 5 部电台, 每台做 1400 小时的试验, 不允许出现一次故障, 才算产品合格。

6.2.2 可靠性增长测定试验

可靠性增长测定试验又称可靠性增长摸底试验, 是我国可靠性工程界根据工程的实际需要自创的一种试验方法。



如前所述,产品可靠性指标的测定试验一般都采用较长时间的寿命考核方法进行。若按 GJB 1407 规定的可靠性增长试验的要求和方法,可靠性增长试验规定的试验截尾时间也很长,长达 MTBF 要求值的 5~25 倍,因此需要寻找一种试验时间短、效率高的方法,以提高产品的可靠性水平或对产品的可靠性水平做出评估。可靠性增长测定试验就是一种能够满足上述要求的试验方法。这种试验的目的是在产品可靠性鉴定试验前,用最短的时间在综合环境应力条件下,暴露产品的潜在缺陷,并及时采取相应措施,以使产品的可靠性水平得到初步增长,同时,对产品的可靠性水平做出初步评估,以确保其顺利通过可靠性鉴定试验,并为产品以后的可靠性工作提供信息。

1. 试验时机

根据可靠性增长测定试验的目的和作用,试验时机应放在产品大规模研制阶段的中后期,在已经完成了环境应力筛选试验、成功地通过了性能检验试验和环境试验之后,在进行产品质量评审和产品鉴定之前,主要考虑以下几方面理由:

① 可靠性增长测定试验的受试产品应完成了 ESS,度过了早期失效期,已步入偶然失效期,否则,试验结果不能反映产品的真实可靠性水平。

② 可靠性增长测定试验的受试产品应成功地通过在正常环境条件下的性能检验,产品的功能已经齐全。如果连检验都未通过,规定的功能还不具备,显然就谈不上可靠性。

③ 可靠性增长测定试验的受试产品应圆满地通过了环境试验,证明产品在规定的极限环境条件下能正常工作。否则,即使通过了可靠性试验,当环境试验通不过时,必须改设计,那么又要再做可靠性试验。这显然是不可取的。

④ 在可靠性增长测定试验中,如发现故障,要分析原因、更改设计,以便实现产品可靠性增长,所以,本试验必须在更改设计不受限制的阶段实施,也就是说,必须在产品鉴定定型之前实施。

⑤ 可靠性指标是产品的主要技术指标之一,是产品质量评审的重要内容。可靠性增长测定试验报告应作为产品鉴定的必备资料项目,因此,本试验必须在产品质量评审和产品鉴定之前完成。

2. 试验条件

试验条件包括产品的工作条件 and 环境条件。在进行可靠性增长测定试验时应正确模拟这些条件。

在试验期间采用的环境条件及其随时间变化的情况,应能反映产品在现场使用和任务环境的特征,应尽量模拟现场使用的综合环境条件。如果试验设备条件不具备,可选择几项环境条件局部综合及单项环境条件逐次相加。

在环境条件类型的选择上,应考虑到环境条件对产品可靠性影响程度的不同,仅将几个对可靠性影响最大或较大的环境条件局部综合及单项环境条件逐次叠加即可。

在环境条件类型的选择上,应考虑到环境条件对产品可靠性影响程度的不同,仅将几个对可靠性影响最大或较大的环境条件作为试验条件。通常采用电压、温度、振动、湿度等4种环境条件,其他影响较小的环境条件可暂时不予考虑。

在环境条件应力大小等级的选择上,应参照产品在现场实际工作中经常遇到的典型环境应力,而不应使用极值应力。

为了便于在试验中实施操作及监控,应将各个应力及其变化按时间关系进行安排,即设计一个试验环境剖面,并把试验环境剖面划分为若干个周期。

在设计试验环境剖面时,在各个应力的施加次序及时间的确定上,应大体上模拟任务环境中各个应力出现的顺序及作用的时间比例。为了考虑具有工程可实践性,在应力等级的数量上,应进行适当归并和工程处理,不应档次过多。比如,只取3个等级——最高值、最低值、加权平均值。在应力作用时间上也应进行适当集中和工程处理,不应分段过细,比如,其应力在一个等级量值上可加长时间,相对集中施加。对于一些作用时间短的极端严酷量值的应力,可以适当删去,由环境试验中考核。

3. 试验时间

应根据以往试验故障的发生情况,以及新研产品在设计中可靠性工作的开展情况,来确定产品可靠性增长摸底试验的时间。

(1) 根据同类产品以往试验时故障发生的情况确定

从以往电子产品可靠性试验的故障分布可以得到以下结论:产品在某一时刻前可能发生故障的频次较高,以后将逐渐减少;对于不同年代和不同情况下设计的产品,这一时刻是不相同的,其原因如下:

① 早年研制的电子产品,尚未开展可靠性设计,且当时的电子元器件的可靠性水平较低,产品总体的可靠性水平也较低,因而约在前80h就暴露了将近50%的故障。

② 近年来研制的电子产品,虽未开展可靠性设计,但此时电子元器件的可靠性水平已有所提高,产品在投入可靠性试验前经过了严格的环境应力筛选试验,因此,产品暴露绝大部分潜在故障的时间延长到了约300h。

③ 最新研制的电子产品,因进行过可靠性设计,且选用了大量高质量的电子元器件,产品本身的可靠性水平较高,而且在试验前均进行了严格的环境应力筛选,因此,在160h的摸底试验中基本无故障。

从以上分析可以看出,产品发生故障频次较高的这一时间,同产品是否开展了

可靠性设计、元器件的可靠性水平、产品本身的固有可靠性水平、试验前是否进行了环境应力筛选等因素有关。新产品的这一时间明显长于老产品。

(2) 根据新研产品可靠性设计情况确定

新研电子产品从一开始就要开展可靠性设计，产品中使用的元器件的质量水平高，从而产品固有可靠性水平可能较高，且根据现有可靠性试验标准及有关文件要求，产品可靠性增长摸底试验前均需进行环境应力筛选，因此，可以认为新研电子产品的可靠性增长摸底试验时间可能较长。在确定这一时间时，应考虑产品的固有可靠性水平和电子产品研制阶段结束时的最低可接受值两个因素。

- 考虑产品的固有可靠性水平。经验表明，当考虑产品固有可靠性水平，确定产品可靠性增长摸底试验的时间时，可按产品可靠性增长的起始点值，即初始的可靠性水平（也就是预计值，由于该值的误差较大，一般按规定值）的10%选取。
- 考虑产品研制阶段结束时可靠性的最低可接受值

根据可靠性保证试验的基本理论，当产品验证的可靠性值在0.212倍（即研制阶段结束时的最低可接受值）之内无故障时，可以认为该产品具有要验证的可靠性水平。

因此，当考虑产品研制阶段结束时的最低可接受值时，产品可靠性摸底试验时间可按产品研制阶段结束时的最低可接受值的21.2%确定。

(3) 综合确定产品的可靠性增长摸底试验时间

根据经验和有关规定，产品可靠性的预计值一般应高于规定值的25%，门限值约为规定值的80%，研制阶段结束时的最低可接受值约为门限值的60%。由此可以得出，产品研制阶段结束时的可靠性最低可接受值约为预计值的48%，所以，可靠性增长摸底试验时间一般为产品可靠性规定值的10.176%。而考虑产品预计值时的可靠性增长摸底试验时间为10%，因此，两个因素确定的可靠性增长摸底试验时间基本一致。

4. 试验结论

按上述方法在确定的试验时间内完成试验后，可能会出现以下情况，结论如下：

- ① 如果试验过程中未发生故障（故障数 $N=0$ ），则可初步证明，产品可能具有预计的固有可靠性水平（规定值），以及可能具有研制阶段结束时要求的可靠性水平。
- ② 如果试验过程中发生的故障数较少（故障数 $0 < N \leq 2$ ），且经采取有效的纠正措施后未再发生故障，则也可初步证明，产品可能具有预计的固有可靠性水平，以及具有研制阶段结束时要求的可靠性水平。
- ③ 如果试验过程中发生的故障数较多（故障数 $N > 3$ ），则可初步证明产品的可

靠性水平较差，需要对产品进行可靠性分析或安排专门的可靠性增长试验。

5. 参数估计方法

由于在可靠性增长摸底过程中有可能发生大量故障，也可能故障数较少或未发生故障，对发生的故障有的采取纠正措施，有的未采取纠正措施，因此，应针对不同的试验结果采取不同的评估方法。

(1) 试验过程中未发生故障

在无故障情况下，置信水平 γ 为 MTBF 的置信下限为：

$$\theta_L = \frac{2T}{\chi^2_{2,\alpha}} \quad (6-6)$$

式中： θ_L ——规定置信度水平下的 MTBF 的置信下限；

T ——可靠性增长摸底试验时间；

α ——显著性水平， $(1-\alpha)$ 为置信度；

$\chi^2_{2,\alpha}$ ——自由度为 $(2, \alpha)$ 的 χ^2 分布。

(2) 试验过程中发生少量故障

① 对故障采取纠正措施。

如果试验中发生的故障数较少（小于或等于 2），且采取了纠正措施，经专家评审认为纠正措施有效后，其 MTBF 点估计值可按下式计算得出：

$$\hat{\theta} = \frac{T}{1} \quad (6-7)$$

规定置信度水平的区间估计按下式计算得出：

$$\frac{2T}{\chi^2_{\alpha/2,4}} \leq \theta \leq \frac{2T}{\chi^2_{1-\alpha/2,2}} \quad (6-8)$$

② 对故障未采取纠正措施。

如果在试验过程中未对故障采取纠正措施或纠正措施无效，则 MTBF 点估计按下式计算得出：

$$\hat{\theta} = \frac{T}{r} \quad (6-9)$$

式中， r 表示故障数。

规定置信度水平的区间估计按下式计算得出：

$$\frac{2T}{\chi^2_{\alpha/2,2r+2}} \leq \theta \leq \frac{2T}{\chi^2_{1-\alpha/2,2r}} \quad (6-10)$$

如果在试验过程中发生的故障数较多（故障数大于或等于 3 个），且均采取了纠正措施，产品的 MTBF 估计值可按杜安模型计算得出，其区间估计可按 AMSAA

模型计算得出。

6.3 可靠性验证试验

可靠性验证试验的目的是验证产品的可靠性是否达到规定的要求。

可靠性验证试验根据产品的性质分为可靠性鉴定试验和可靠性验收试验。

- 鉴定试验是为了验证新开发产品的设计是否达到规定的最低可接收的可靠性定量要求。
- 验收试验是对正式转入批生产产品是否达到可靠性定量要求的试验。

可靠性验证试验，从试验原理来说，需要应用统计抽样理论，因此又称统计试验。其目的是为了验证产品是否符合规定的可靠性要求，由承制方根据有关标准、研制生产进度制订方案和计划，经定购方认可。验证试验包括产品研制的可靠性鉴定试验和批量生产的可靠性验收试验。这类试验必须能够反映装备的可靠性定量水平，因此试验条件要尽量接近使用的环境应力；试验结果要给出接收或拒收的判断，因此对试验时间和发生的故障应进行详细记录，经过与失效判据的对比分析后，试验各方统一认识后才能给出最后的结论。

6.3.1 抽样检验

1. 抽样检验的分类

可靠性验证试验属于统计试验，制订试验方案时需要确定抽样方案。抽样检验方案可按其性质、用途、抽样次数以及实施方式等进行分类，下面分别予以介绍。

(1) 按性质分类

抽样检验按其性质可以分为计数抽样检验方案和计量抽样检验方案。

① 计数抽样检验方案。

它是指从一批产品中抽取一定数量的样品进行检验，将检验样品分为合格品和不合格品两类，然后将检验出的不合格品数与事先规定的“合格判定数”进行比较，来判断该批产品是否合格。这种检验只统计样品中的不合格品个数，而不对每一样品的参数值进行统计。

② 计量抽样检验方案。

它是指从一批产品中抽取一定数量的样品，按计量的方法检验样品的某一质量指标（如电阻的阻值，仪器的平均寿命等），并与规定的技术标准进行比较，以判

断整批产品质量合格与否，这种方案就是计量抽样检验。

计量抽样与计数抽样相比，对每一样品的考察较为细致，充分利用了子样提供的信息，因而可以用较少的样品对总体进行较准确的推断。但是计量抽样方案涉及产品的具体参数，而且要事先对产品参数的均值和方差进行必要的统计，所以这一类抽样方案作为通用的抽样标准较为困难，主要适用于特定产品的检验，尤其适用于制造过程中的质量控制。尽管产品的质量特征是可以定量地衡量，即可用计量抽样进行检验，但为了节省检验的时间、人力和物力，而采用计数抽样检验方案。

（2）按抽样次数分类

抽样检验按其抽样次数可以分为一次抽样检验、二次抽样检验、多次抽样检验和逐次抽样检验。

① 一次（单式）抽样检验。

一次抽样检验的一般过程是先从总数为 N 的一批产品中（有时 N 是未知数）随机抽取 n 个样品（ $n < N$ ），然后对这 n 个样品进行检验（或试验）。将次品（故障）数记为 r ，与事先确定的合格判定数 c 进行比较，若 $r \leq c$ 则认为整批产品合格；反之则为不合格（见图 6-5）。因此一次抽样方案的核心，就是如何在事先确定抽样数 n 与合格判定数 c ，这就是抽样方案的制订问题。

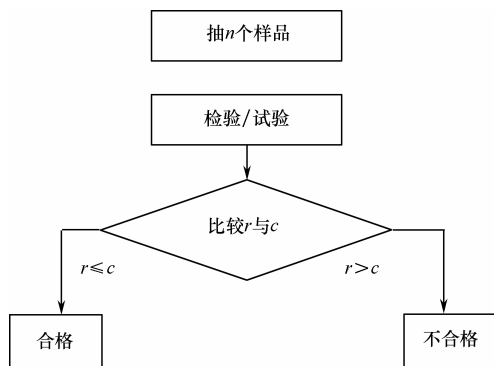


图 6-5 一次抽样检验程序

② 二次（复式）抽样检验。

它是根据第一次样品检验的结果，判断整批产品合格、不合格或还不能做出判断，而需要抽取第二次样品。再根据第二次样品的检验结果，加上第一次样品检验结果，判断整批合格或不合格。

③ 多次抽样检验。

它是指如果抽取第一次样品和第二次样品后，其检验结果还不能做出是否合格的判断时，应继续抽取样品进行检验，直到能根据所抽样品的试验结果判断出该批产品是否合格为止。



④ 逐次抽样检验。

其也称序贯抽样检验，与多次抽样检验不同的是这种方法每次只从整批产品中抽取一个产品，当抽取了 k 次以后有不合格品 r_k 个，合格品 $k-r_k$ 个。计算产品出现这个抽样检验结果的概率情况，以做出接收、拒收整批产品或继续试验的判决。 k 可以是 1, 2, 3……视判决需要而定。

一次抽样方案简单，手续方便，最容易为人们所掌握，所以应用较广。但与二次和序贯抽样相比，在检验精度相当时，抽样数量最多。通常用于产品数量较大、检验费用不太高的场合。序贯抽样的检验手续和方案制订都比较复杂，但能节省样品。二次抽样则介于一次和序贯抽样之间，是一种常用的抽样方法。

(3) 按用途分类

抽样检验按其用途可分为质量检验和可靠性检验。

① 质量检验。

它是为了保证产品质量而进行的抽样检验，如对外购原材料、元件、配件等进行的入库检验，对生产流程中的工序工艺检验，对产品进行例行检验，对成品或半成品的入库检验，以及出厂的交收检验等。

② 可靠性检验。

它是为了检验产品的可靠性而进行的抽样检验，如寿命抽样检验或失效率抽样检验等。

(4) 按实施的方式分类

可分为逐批抽样检验、连续抽样检验、调整型抽样检验和筛选型抽样检验方案。

① 逐批抽样检验方案。

它是指从需要检验的一批产品中抽取一定数量的样品，根据样品检验的结果来判断此批产品是否合格，决定接收还是拒收此批产品。

② 连续抽样检验。

它是指在生产线上的某一指定的检验点直接检验产品。按照选定的连续抽样检验方案，通过交替地使用抽样检验和逐个检验来保证一定的产品质量，即在开始时逐个检验通过预先指定的某一检验点的每个产品。如果接连 i 个产品都合格，接下去采用抽样检验，在相邻的每 j 个产品中任抽取 k 个进行检验，如果全合格，则继续采用抽样检验，一旦出现不合格产品，立即恢复逐个检验。在整个检验过程中，以合格品替换在检验中发现的不合格品，替换的手续可以在检验进行到一个阶段时进行。

③ 调整型抽样检验方案。

在连续生产的情况下，根据产品质量的好坏变化或以往若干批检验的结果，随时调整检验的严格程度。它可分为正常检验、从严检验以及从宽检验等三种情况。

当产品质量比较正常时,采用正常抽样检验方案;当产品质量变劣时,改用加严的抽样检验方案;当以往检验的结果说明产品质量较好时,可以采用放宽的抽样检验方案。把正常的抽样检验、加严抽样检验和放宽抽样检验用一套调整的规则联系起来,这就是调整型抽样检验方案。

④ 筛选型抽样检验方案。

它也是一种非调整抽样检验方案。它的特点是:对不合格批产品进行百分之百的筛选,剔除不合格品,补足原有批量数后再次提交检验,从而使不合格批产品变成合格批产品给予出厂。显然,筛选型抽样检验不适宜破坏性检验的场合。

以上介绍了各种抽样检验方法,它们各有用处。最常用的是一次计数抽样方法。

2. 接收概率与抽样特性曲线

一批产品按某一抽样检验方案进行检验而被判为合格的概率称为该抽样检验方案的接收概率,显然,接收概率与该批产品的产品质量次品率 P 有关,所以记作 $L(P)$, $L(P)$ 也称为抽样检验的特性函数。

首先考虑一次抽样检验方案 $\{n, c\}$ 与产品质量的关系。设产品的次品率为 p , 良品率 $q=1-p$, 在样本量为 n 的样品中,可能出现 r 个次品的概率为

$$P(n, r | p) = \binom{n}{r} p^r q^{n-r} \quad r=0, 1, 2, \dots, n \quad (6-11)$$

其中,二项系数 $\binom{n}{r} = \frac{n!}{(n-r)!r!}$, 而 $\binom{n}{0} = 1$ 。当 n 较大时,式(6-11)可由下式近似得到:

$$P(n, r | p) = \frac{(np)^r}{r!} e^{-np} \quad (6-12)$$

根据检验程序,当出现任意 $r \leq c$ 时,都认为产品为合格,可以接收该产品,因此称 $L(p)$ 为方案 $\{n, c\}$ 的接收概率,即

$$L(p) = \sum_{r=0}^c P(n, r | p) \quad (6-13)$$

显然,对于一个确定的抽样检验方案 $\{n, c\}$, 当产品质量不一样时其接收概率也是不一样的。例如,对于一个 $\{20, 2\}$ 的检验方案,当被检验的产品,其次品率分别为 1%、5%、10%、15%、20%、25%、30%、40% 或 50% 时,按如图 6-5 所示的程序,经过抽样检验,产品被接收的可能性 $L(p)$ 分别为:

$$\begin{array}{lll} L(1\%)=0.9990 & L(5\%)=0.9245 & L(10\%)=0.6769 \\ L(15\%)=0.4049 & L(20\%)=0.2061 & L(25\%)=0.0913 \end{array}$$

$$L(30\%)=0.0208$$

$$L(40\%)=0.0020$$

$$L(50\%)=0.0002$$

若将 $L(p)$ 值与次品率 p 用函数曲线画出，就可得到该检验方案的抽样特性曲线，即 OC 曲线（见图 6-6）。

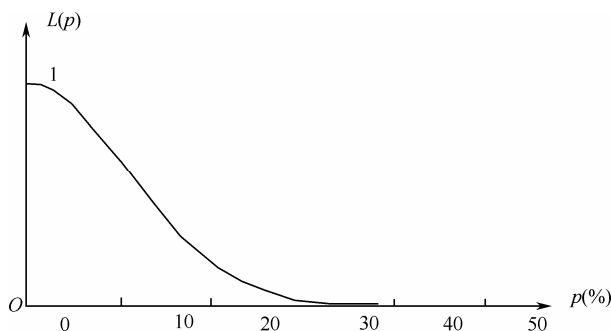


图 6-6 方案 $\{20, 2\}$ 的 OC 曲线

由此可见，当采用上述方案对产品实施抽样检验时，不同质量的产品实际上都有通过检验的可能，即出现 $r \leq c$ 的情况，而被判为合格，只不过被判的概率有大有小而已。换句话说，当采用抽样方法对产品质量进行检验时，再差的产品也有被判为合格的可能；而再好的产品也有被判为不合格的可能，出现这种情况，我们称之为“误判”，这就是抽样检验存在的两类错误。

6.3.2 可靠性验证试验大纲要求

1. 试验大纲内容

试验大纲覆盖以下内容：

- ① 试验对象和数量。
- ② 试验目的、进度。
- ③ 试验方案。
- ④ 试验条件：试验设备提供的应力及其容差；检测设备及其精度要求。
- ⑤ 试验场所，经订购方认可按以下顺序选定：独立实验室，合同乙方以外的实验室，合同乙方的实验室。
- ⑥ 设置评审点、开展 FRACAS 要求。

2. 试验方案

(1) 试验方案的内容

根据大纲要求制订试验方案，内容包括：

① 试验项目。

② 选定统计试验方案：号码、鉴别比 D 、风险 α 和 β 、试验时间 T 、样品数量、是否可替换。

③ 试验剖面。

④ 故障判据及分类。

⑤ 有关试验方职责分工。

⑥ 计划进度、经费、人员、维修器材等资源保证条件。

⑦ 其他可靠性活动信息。

(2) 试验方案的选定因素

确定试验方案时，应考虑下列因素：

① 定时截尾试验，累积试验时间是确定的，便于试验计划的安排和管理，但不一定是最经济的。

② 定数截尾试验，累计相关故障数是确定的，在采取不可替换的试验时，样品数量是不确定的，也不一定是最经济的。

③ 等概率比序贯试验，做出判据所需的故障数和累计试验时间，比定时截尾和定数截尾试验少，事前只能确定它们的最大值，但样品数量和试验时间难以确定，不便于试验计划的安排和管理，最大累积试验时间和累计故障数有可能超过定时截尾或定数截尾的试验。

3. 试验条件

可靠性验证试验剖面应典型代表产品的使用条件：

① 功能模式，当产品有超过一种使用模式时，应分析各自所占时间的百分比，确定模式转换的方式，提出试验用典型工作模式。

② 输入信号，试验中测试设备向样品输入一系列信号，使样品正常工作。

③ 负载条件，样品输出端应模拟使用状态加载，测试样品输出性能。

④ 样品操作，试验中由产品操作人员模拟使用状态进行操作。

⑤ 保障条件，实验室提供的电源、水源、气源等的各项参数应符合要求。

⑥ 试验剖面，尽量采用综合应力试验设备模拟产品使用条件，同时对样品施加温度、湿度、振动、低气压等应力。

⑦ 样品维护和修理，试验大纲可能规定样品有定期维护的程序，应按照产品使用说明正常维护，不得改变其技术状态；样品发生故障时，应准予修理，由承制方保证条件并实施，不得改变样品技术状态。

4. 试验程序

应根据试验方案制订试验程序，经订购方审批后作为落实试验计划的文件，内

容包括:

- ① 试验过程。
- ② 样品及其技术状况。
- ③ 需检测的特性参数、故障判据及其容限、检测时段及方法。
- ④ 综合环境条件及其容差。
- ⑤ 试验日志及记录的数据内容、记录时间间隔要求。
- ⑥ 故障记录表格及其登记内容、分析报告要求。

5. 试验评审

试验评审包括: 试验大纲评审、试验方案评审、试验程序评审、试验准备状态评审、试验中评审、试验完成综合评审。前 4 项评审可以结合在一起进行, 必须有订购方代表参加; 试验中的评审视情况进行, 如对故障处理和试验进度、序贯试验终结与否进行评审, 由试验现场负责人组织实施; 试验完成综合评审, 应在试验报告编制完成之后进行, 评价试验结果、产品可靠性水平及其接收与否的结论、FRACAS 报告、问题处置和纠正措施的落实等。

6. 试验报告要求

试验报告是产品可靠性水平的正式记录, 包括试验中产生的各种原始记录、试验结果的处理报告和结论意见。

6.3.3 平均寿命抽样检验的原理与试验方案

在可靠性工作中, 人们所关心的质量指标是产品的失效率、平均寿命、可靠寿命等, 虽然这些指标是连续变量, 可以用“计量”方法来衡量, 但正如前面所提到的, 是为了方便我们采用“计数”方法。需要指出的是为了检验这些指标必须进行寿命试验, 而且寿命试验往往是截尾的。假定产品的寿命分布是单参数指数分布, 其分布函数为:

$$F(t) = 1 - e^{-\lambda t} = 1 - e^{-\frac{t}{\theta}} \quad (t \geq 0)$$

其中, $\lambda > 0$ 是产品的失效率, $MTBF = 1/\lambda$ 是产品的平均寿命, 均为未知参数。在试验中, 常用 θ (GJB 899A) 或 m 表示 MTBF, 在下面的叙述中用 θ 表示 MTBF。

对于大部分电子设备我们都以指数分布的假设来描述其寿命分布, 并鉴于电子设备发生故障后通常是可修复的, 因此可采用 MTBF (即平均故障间隔时间) 来反映其可靠性水平。然而在制订 MTBF 值的抽样试验方案时, 必须对前面采用的计数

抽样方案进行必要的变换。

合格平均寿命 θ_0 是指当产品平均寿命 $\theta \geq \theta_0$ 时, 产品是符合要求的, 应以高概率接收, 即要求 $L(\theta_0)=1-\alpha$, 也就是当 $\theta \geq \theta_0$ 时, $L(\theta_0) \geq 1-\alpha$ 。不合格平均寿命 θ_1 是指当产品的平均寿命 $\theta \leq \theta_1$ 时, 产品不符合要求, 应该以低概率接收, 即要求 $L(\theta_1)=\beta$, 也就是当 $\theta \leq \theta_1$ 时, $L(\theta_1) \leq \beta$ 。

在式 (6-12) 中 np 代表了在样本为 n 的样品中存在的次品的平均分数。对于可靠性试验, 可以证明, 当产品的寿命服从指数分布, 其平均故障间隔时间 $MTBF=\theta$ 时, 在总累积试验时间 T 内, 其发生故障的平均次数为 $r=T/\theta$, 因此, 参照式 (6-12), 我们可以得到在总试验时间 T 内, 发生 r 次故障的概率为:

$$P(T, r | \theta) = \frac{(T/\theta)^r}{r!} e^{-T/\theta} \quad (6-14)$$

参照式 (6-13), 可以得到可靠性鉴定试验方案 $\{T, C\}$ 的接收概率:

$$L(\theta) = \sum_{r=0}^c P(T, r | \theta) \quad (6-15)$$

应注意的是这里的方案 $\{T, C\}$ 构成了一个“定时截尾”方案, 而不是原来的 $\{n, c\}$ “计数抽样”方案。

为了使构造的定时截尾可靠性鉴定试验方案, 能够控制给供货方和订购方带来的风险 (亦即“生产方风险” α 和“使用方风险” β), 我们要求方案 $\{T, C\}$ 必须满足:

$$\begin{cases} L(\theta_0) = 1 - \alpha \\ L(\theta_1) = \beta \end{cases} \quad (6-16)$$

$$\text{即: } \begin{cases} \sum_{r=0}^c P(T, r | \theta_0) = 1 - \alpha \\ \sum_{r=0}^c P(T, r | \theta_1) = \beta \end{cases} \quad (6-17)$$

这里, θ_1 代表产品 MTBF 的最低可接受值, 亦称检验下限, 当产品的可靠性真值达到此下限值时, 试验方案仅以较小的概率 β , 对其做出“接收”判决; θ_0 代表产品 MTBF 的可接受水平, 亦即检验上限, 当产品的可靠性真值达到此上限值时, 试验方案将以较高的概率 $1-\alpha$ 对其做出“接收”判决, 而被误判为“拒收”的概率仅为 α 。 $D_m=\theta_0/\theta_1$ 称之为鉴别比。显然 α 、 β 值越小, D 的值越接近于 1, 则试验方案 $\{T, C\}$ 的特性曲线越接近于理想 (见图 6-7)。

常用于设备可靠性鉴定的统计试验方案, 其 α 和 β 一般取 10%、20%或 30%; 鉴别 D_m 值一般约为 1.5、2 或 3。表 6-6 给出了国标 GB 5080.6 和国军标 GJB 899A 中推荐的设备可靠性鉴定常用的标准型定时截尾统计试验方案, 而这些方案所具有



的 OC 曲线, 标准中已详细给出。在拟定试验方案时, 应根据规定的产品 MTBF 最低可接受值 θ_1 、供货方认定的 θ_0 , 以及双方承担的试验风险 α 和 β (可以相等, 也可以不等), 并根据进行鉴定试验能投入的人、财、物条件, 如样品数、试验时间、试验设备和试验经费等, 科学合理地选定统计试验方案。

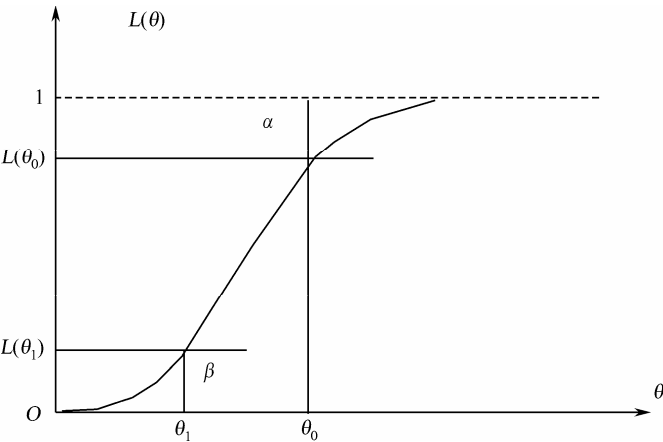


图 6-7 试验方案 $\{T, C\}$ 的典型 OC 曲线

表 6-6 GJB 899A 的标准型定时截尾试验方案

方案号	决策风险（%）				鉴别比 $D_m=\theta_0/\theta_1$	试验总时间 T （ θ_1 的倍数）	合格判定 责任故障 数 C
	名义值		实际值				
	α	β	α'	β'			
1-1	10	10	12.0	9.9	1.5	45.0	36
1-2	10	20	10.9	21.4	1.5	29.9	25
1-3	20	20	19.7	19.6	1.5	21.5	17
1-4	10	10	9.6	10.6	2.0	18.8	13
1-5	10	20	9.8	20.9	2.0	12.4	9
1-6	20	20	19.9	21.0	2.0	7.8	5
1-7	10	10	9.4	9.9	3.0	9.3	5
1-8	10	20	10.9	21.3	3.0	5.4	3
1-9	20	20	17.5	19.5	3.0	4.3	2
1-10	30	30	29.8	30.1	1.5	8.1	6
1-11	30	30	28.3	28.5	2.0	3.7	2
1-12	30	30	30.7	33.3	3.0	1.1	0

当产品采用定时截尾方案完成试验考核, 得到“接收”或“拒收”的结论后, 对产品实际达到的可靠性水平, 仍可采用在可靠性测定试验中介绍的数据处理方

法，对产品的 MTBF 给出点估计和区间估计。区间估计的置信度在原则上可任意选定，但对于鉴定试验后的 MTBF 估计，其下限估计置信度，一般建议取 $c=1-\beta$ ，而双边估计置信度取 $c=1-2\beta$ ，其理由是为了使估计结果与鉴定结论相一致。

表 6-7 是 IEC 60605-7 《设备可靠性验证试验方案》中所规定的抽样方案。表中的截尾时间是总试验时间，注意它是 θ_0 的倍数，鉴别比用 D_m 表示，当试验截止时，合格判定数应是表中截尾失效数减 1。

表 6-7 IEC 60605 的定时定数截尾试验方案

方案编号	方案的特征			截尾时间 (θ_0 的倍数)	截尾失效数	实际的风险 (%)	
	标 称 值 (%)		D_m			$\theta=\theta_0$	$\theta=\theta_1$
	α	β				α_1	β_1
1.1	10	10	1.5	30.0	37	12.0	9.9
1.2	10	10	2	9.4	14	9.5	10.6
1.3	10	10	3	3.1	6	9.4	9.9
1.4	10	10	5	1.10	3	10.0	8.8
1.5	20	20	1.5	14.1	18	18.0	21.7
1.6	20	20	2	3.9	6	20.0	21.0
1.7	20	20	3	1.46	3	18.1	18.8
1.8	30	30	1.5	5.3	7	28.3	32.0
1.9	30	30	2	1.84	3	28.0	28.9
1.10	35	40	1.25	6.7	8	35.7	40.3

【例 6-5】制订试验方案

在 $\alpha=\beta=10\%$ ， $\theta_1=5000h$ ， $D_m=3$ 的条件下，制订某仪表的平均寿命验证试验方案。

解：由题意可得 $\theta_0=D_m\theta_1=15000h$ 。

查表 6-7，可选用编号为 1.3 的方案。总试验时间需要 $T=3.1\theta_0=46500h$ 。当试验停止时，仪表的失效数 $r<6$ 时，可接收该批仪表；当 $r\geq 6$ ，则拒收该批仪表。

一个值得注意的问题是：进行定时截尾可靠性鉴定试验时，在统计试验方案选定后，一旦正式投入试验，那就不允许中途改变原定的试验方案。例如，原定试验按表 6-7 中方案 1.6 即 $\{T=7.8\theta_1, C=5\}$ 进行，但当试验时间至 $4.3\theta_1$ 时，产品仅发生过 1 次故障，于是认为若变为按表 6-7 中方案 1.9 $\{T=4.3\theta_1, C=2\}$ 评估，则可对产品给出“合格”判定，故为节省时间与经费，试验不再继续。又如原已按方案 1.9 $\{T=4.3\theta_1, C=2\}$ 进行，而试验还未进行到 $4.3\theta_1$ 时，已发生 3 次故障，这时，本应做出“不合格”判定，但经协商同意，继续按方案 1.6 $\{T=7.8\theta_1, C=5\}$ 延长试验。然而这两种做



法都是违反定时截尾统计试验规则的，在实际使用中是不允许的！

针对上述违规做法，在国军标 GJB 899A 中介绍了一种在进行定时截尾试验时，根据产品发生故障的时间，可给出提前“接收”的定时截尾试验方案；另外，在国标 GB 5080.6 和国军标 GJB 899A 中，还给出了一种可根据试验的具体进程，随时给出“接收”或“拒收”判定的序贯截尾统计试验方案。

6.4 环境应力筛选（ESS）

6.4.1 环境应力筛选的目的

环境应力筛选的目的在于发现和排除产品的早期失效，使其在出厂时便进入随机失效阶段，以固有的可靠性水平交付用户使用。

研制阶段一般按照经验得到的筛选方法进行常规筛选，其主要作用是：一方面用于收集产品中可能存在的缺陷类型、数量及筛选方法效果等信息；另一方面，在可靠性增长和工程研制试验前进行了常规试验，可节省试验时间和资金，同时有利于设计成熟快捷的研制试验方法。

研制阶段的常规筛选要为生产阶段的定量筛选收集数据，为定量筛选做准备，设计定量筛选的大纲。

生产阶段的筛选主要是实施研制阶段设计的定量筛选大纲，并通过记录缺陷析出量和设计估计值的比较，提出调整筛选和制造工艺的措施，参考结构和成熟度相似的产品定量筛选经验数据，完善或重新制订定量筛选大纲。

6.4.2 环境应力筛选的原理

环境应力筛选通过向电子装备施加合理的环境应力和电应力，将其内部的潜在缺陷加速变成故障，以便人们发现并排除。

环境应力筛选是装备研制生产的一种工艺手段，筛选效果取决于施加的环境应力、电应力水平和检测仪表的能力。施加应力的大小决定了能否将潜在的缺陷在预定时间内加速变为故障；检测能力的大小决定了能否将已被应力加速变成故障的潜在缺陷找出来，以便加以排除。因此，环境应力筛选又可看做是产品质量控制检查和测试过程的延伸，是一个问题暴露、识别、分析和纠正的闭环系统。对电子产品而言，环境应力筛选主要是在产品上施加随机振动及温度循环应力，以鉴别和剔除产品工艺和元件引起的早期故障的一种工序或方法。它可以加速暴

露装配和制造缺陷。环境应力筛选的对象既包括元器件级,也包括组件级、分机级、系统级产品。实践证明,环境应力筛选是可以有效暴露电子组件、设备中的元器件和制造工艺缺陷的方法,因此应作为必要的一道制造工序。根据国外所提供的数据,环境应力筛选可减少现场失效率 20%~90%,大大减少寿命周期总费用,可减少生产厂内失效率达 75%,大大减少生产成本,因此,环境应力筛选应对 100%的电子产品进行。

6.4.3 试验剖面的确定

1. 应力类型

定量环境应力筛选一般选用温度循环和随机振动应力,对电子产品而言,一般都可以满足筛选要求。某些产品有特殊要求的可选用特定的筛选应力。

2. 应力组成

温度循环和随机振动应力各自激发的缺陷类型是不相同的,因此不能互相取代。然而,它们在激发缺陷的能力上却可以互相补充和加强,由振动加速发展的缺陷可能在温度循环中以故障的形式暴露出来,同样,由温度循环加速发展的缺陷也可能在振动中以故障形式暴露出来,因此,环境应力筛选的试验剖面应把温度循环和随机振动组合起来,即随机振动—温度循环—随机振动或温度循环—随机振动—温度循环。可以参阅 GJB 1032《电子产品环境应力筛选方法》。

3. 应力量值

筛选应力的量值以不能超过产品的设计极限,激发潜在缺陷又不损坏产品中完好的部分为原则。

(1) 温度循环参数的选择

① 确定温度循环的上下限温度。

采用加电检测性能的筛选方案时,温度循环的上下限温度不高于和低于设计的最高和最低的工作温度。

采用非加电检测性能的筛选方案时,温度循环的上下限温度不高于/低于产品储存的高温/低温。

采用只在上限(或下限)温度加电和检测性能的筛选方案时,温度循环的上限(或下限)温度不高于(不低于)设计的最高(最低)工作温度,另一侧的温度不低于(或高于)储存温度,如图 6-8 所示。

只对组件进行筛选时，要找出组件中分组件（元器件）各自的最高和最低工作温度、最高和最低储存温度，温度循环的上下限温度以这些高温中的最低者和低温中的最高者为温度组，参照上述原则进行设计。一般设计的工作温度和储存温度离设计的极限温度还有一定距离，为了提高筛选效率，有时扩大温度变化幅度，向设计的极限温度靠拢。

② 确定温度变化速率。

温度变化速率对筛选效果影响极大，应尽可能加快温度变化速率。标准规定设备或部件筛选的温度变化速率不小于 $5^{\circ}\text{C}/\text{min}$ 。由于受筛选产品本身的热惯性，产品的实际温度变化速率远低于试验箱内的空气温变平均速率，因此要根据试验箱的能力尽量提高温度变化速率。

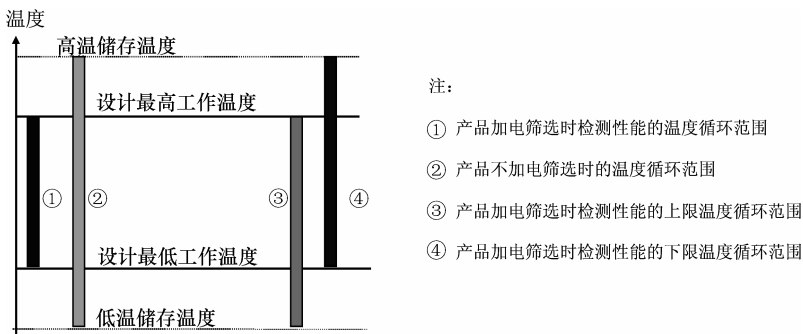


图 6-8 筛选温度范围示意图

在条件不具备，进行非定量环境应力筛选时，可采用两箱法进行温度冲击筛选。在定量环境应力筛选过程中，可按定量要求和观察到的故障数调节已选定的温度变化速率，以保证实现定量目标。

③ 确定上、下限温度的持续时间。

在温度循环中上、下限温度的持续时间取决于产品在此温度下达到稳定的时间和检测性能所需的时间，可在对产品的热测定和对试验箱温度稳定时间的测定后确定。

④ 确定温度循环次数。

温度循环次数实际上就是筛选的持续时间。根据电子设备早期故障一般在交付的前 $50\sim100$ 小时暴露，它与产品的复杂程度有关。一般而言，初始筛选和单元级的筛选采用 $10\sim20$ 个循环，组件级筛选采用 $20\sim40$ 个循环。

(2) 振动应力的选择

① 确定振动量值。

筛选的振动量值一般应低于产品环境鉴定试验的合格值，以不损坏产品为准。

常规筛选的随机振动量值一般可用 $0.04\text{g}^2/\text{Hz}$ ，把握不大的产品可根据通过测定摸清产品对振动的响应特性，由低到高适当调整，最后确定振动量值。

② 确定随机振动频谱。

随机振动频谱应采用 GJB 1032 或 GJB/Z 34 标准规定的频谱，频率范围为 $20\sim 2000\text{Hz}$ ，对少数情况可缩小到 $100\sim 1000\text{Hz}$ 。

应对受筛选产品进行振动测定，确定产品共振频率、优势频率，对产品响应大的频率段要减少输入，反之加大输入，以保证不损坏产品和实施规定量值的筛选。

③ 确定轴向和时间。

随机振动一般要在三个轴向上进行，每个轴向振动 $5\sim 10\text{min}$ ，最少不少于 5min 。如果产品中多数印制板呈同一个方向排列，则可在垂直于印制板方向进行 10min 的随机振动。正弦振动也应在三个轴向上进行，一般进行 30min ，不超过 60min 。

随机振动的最大效果发生在 $15\sim 20\text{min}$ 内，延长振动时间不仅无益于筛选，反而会引起疲劳损伤，一般用 $0.04\text{g}^2/\text{Hz}$ 振动 20min 。

(3) 加电和性能检测时间的选择

① 一般原则。

为保证筛选效果，筛选中应尽量进行加电和性能检测，以便发现间歇故障和电应力缺陷。从可能性和经济性出发，一般在高装配等级筛选时进行间歇加电和性能检测，低装配等级可能不具备性能检测的条件，若专门设计制造一套检测仪表，则费用太大，筛选时只好不进行加电和性能检测。

② 温度循环的加电和性能检测。

为了不影响降温速率，在降温过程中可不加电，为了发现间歇性故障也可加电；尽量在其他温度段加电，期间如果不能连续进行性能检测，也应尽量频繁检测，以便及时发现故障和节省筛选时间。

③ 随机振动的加电和性能检测。

在振动过程中，应加电和进行性能检测，以保证及时发现故障、不漏检间歇故障；如果出现故障后不影响加电和检测，则在振动结束后再修理。

6.4.4 典型的环境应力筛选过程

按 GJB 1032《电子产品环境应力筛选试验方法》(M.S-2164) 环境应力筛选的整个过程包括四道依次进行的工序(见表 6-8)：(1) 初始性能检测；(2) 缺陷剔除试验；(3) 无故障检验；(4) 最后性能检测。下面对各工序进行简要说明。

表 6-8 环境应力筛选过程

初始性能检测		环境应力筛选			最后性能检测	
		缺陷剔除	无故障检验			
		随机 振动	温度 循环	温度 循环	随机 振动	
		40h	40~80h 在80h中应 有40h 无故障			
		40h	80h			
随机振动 5min		温度循环	温度循环	随机振动 5~15min		
		最大限度地监测功能			在15min中应有 5min无故障	

1. 初始性能检测

在进行 ESS 前后，试验产品应按技术规范进行外观、机械及电气性能检测。凡初始检测不合格者不能继续进行环境应力筛选试验。

2. 缺陷剔除试验

对受试产品施加规定的随机振动和温度循环应力，以激发出尽可能多的故障。在此期间，发现的所有故障都应记录下来并加以修复。

在随机振动试验时出现的故障，待随机振动试验结束后排除；在温度循环试验时出现的故障，每次出现故障后，应立即中断试验，排除故障再重新进行试验。

中断处理：试验因故中断后再重新进行试验时，中断前的试验时间应计入试验时间，对温度循环则需扣除中断所在循环内中断前的试验时间。

3. 无故障检验

试验目的在于验证筛选的有效性，应先进行温度循环，后进行随机振动。所施加的应力量级与缺陷剔除试验相同。不同的是温度循环时间增加到（最大为）80h；随机振动增加到（最长为）15min。

在试验过程中应对试验产品进行功能监测，在最长 80h 内只要连续 40h 温度循环期间不出现故障，即可认为产品通过了温度循环应力筛选；在最长 15min 内连续 5min 内不出现故障，即可认为产品通过了随机振动筛选。

4. 最后性能检测

将通过无故障检验的产品在标准大气条件下通电工作，按产品的技术条件要求逐项检测并记录其结果，将最后性能与初始测量值进行比较，对筛选产品根据规定

的验收功能极限值进行评价。

【例 6-6】环境应力筛选案例

某手机微波中继设备,按照环境应力筛选标准 GJB 1032,采用高低温循环和随机振动两种应力组合。

① 温度循环应力可根据设备设计的工作环境温度范围 $+60^{\circ}\text{C}$ 、 -40°C 和试验设备的能力确定:产品通电工作筛选温度范围为 $+60^{\circ}\text{C}\sim-40^{\circ}\text{C}$;温度变化率为 $+7^{\circ}\text{C}/\text{min}$ 、 $-11^{\circ}\text{C}/\text{min}$;根据性能检测要求,确定高、低温停留时间各为 1.5 小时,一个温度循环时间为 3.5 小时;暴露缺陷的循环次数为 10,无故障验收试验循环次数为 20。

② 随机振动应力可按照 GJB 1032 标准的规定和随机振动设备的能力确定:频率范围为 $20\sim 2000\text{Hz}$;功率谱密度为: $0.04\text{g}^2/\text{Hz}$ (在 $80\sim 350\text{Hz}$ 之间); $20\sim 80\text{Hz}$ 和 $350\sim 2000\text{Hz}$ 功率谱密度变化率为 $\pm 3\text{dB}/\text{倍频程}$ (见图 6-9)。

③ 应力施加步骤,即根据 GJB 1032 标准的规定,应力施加的顺序是:随机振动 15 分钟 \rightarrow 温度循环 10 个周期(暴露缺陷过程) \rightarrow 温度循环 20 个周期(无故障验证试验) \rightarrow 随机振动(5~15 分钟)。

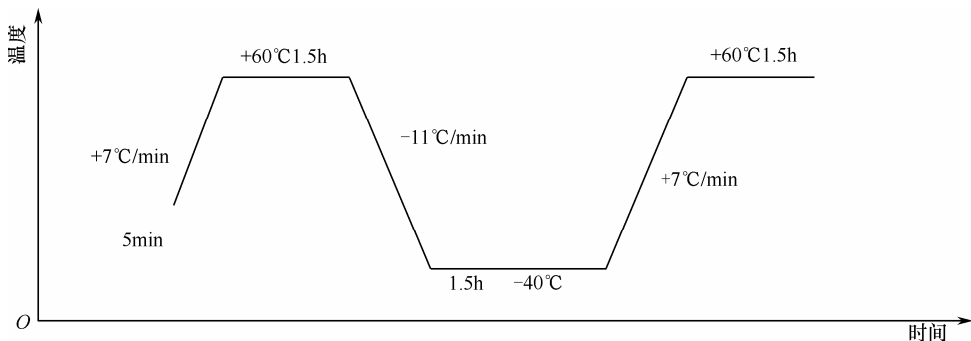


图 6-9 温度循环剖面示意图

④ 温度循环剖面示意图如图 6-9 所示,随机振动谱示意图如图 6-10 所示。

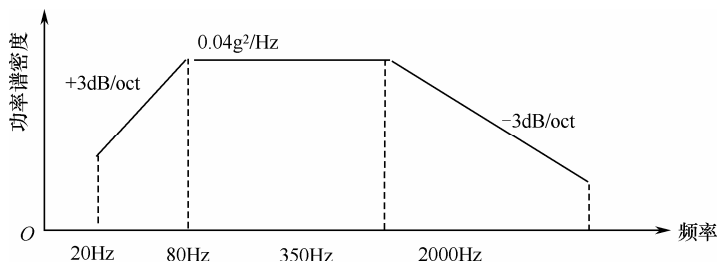


图 6-10 随机振动谱示意图



6.5 可靠性增长试验

6.5.1 可靠性增长试验的内涵及其作用

可靠性增长是通过逐步改正产品设计和制造中的缺陷，不断提高产品可靠性的过程。

在工程研制阶段，可靠性增长试验可使产品更有把握地达到预期的可靠性目标；在使用阶段，可靠性增长可使产品的可靠性有一定程度的提高，改善产品固有的可靠性。

可靠性增长的核心是消除影响产品可靠性水平的设计缺陷。可靠性增长的关键是发现影响产品可靠性水平的设计缺陷。为此，必须通过试验或运行的途径来实现产品故障机理的检测。常见的可靠性增长有一般性的可靠性增长和可靠性增长管理。

- 一般性的可靠性增长，是指事前未给出明确的可靠性增长目标，对产品在设计或运行中发生的故障，根据可用于可靠性增长资源的多少，选择其中的一部分或全部实施纠正措施，以使产品可靠性得到确实提高的过程；它通常不制订计划增长曲线，也不跟踪增长过程，而是采用一两次集中纠正故障的方式，使产品可靠性得到提高。由于增长过程通常不能满足增长模型的限度条件，增长后的产品可靠性水平需要通过可靠性验证试验才能进行定量评估。
- 可靠性增长管理，是指有计划、有目标的可靠性增长工作项目，并非可靠性增长过程中的管理工作。它是产品寿命期内的一项全局性的、为达到预期的可靠性指标、对时间和资源进行系统安排、在估计值和计划值比较的基础上依靠新分配资源、对实际增长率进行控制的可靠性增长项目。

可靠性增长活动是一个连续完整的闭环控制过程。在此环中，首要任务是发现产品的设计缺陷——主要是在试验、使用中发生的故障；然后是对故障进行分析——重点研究重复性故障和关键故障发生的原因，当认定为设计缺陷后提出纠正这些设计缺陷的措施；接着是实施纠正措施——将修改设计的措施在少数产品（试验样品）上实施，并通过试验验证纠正措施的有效性；最后是修改技术文件和把纠正措施推广到同型号产品中去——这是落实可靠性增长活动的重要工作，是发挥可靠性增长试验效益的关键步骤。可靠性增长活动可以在工程研制阶段、生产阶段进行，甚至在使用阶段进行。按照有关标准的规定只在装备研制阶段才进行可靠性增长试验和增长工作，但从我国的实际情况出发，有不少已经装备多年的产品仍然对其进行可靠性增长试验和“可靠性补课工作”，并取得了显著成绩。这就是说，要

根据产品的技术状况和可靠性水平去决定何时以何种形式开展可靠性增长活动。

可靠性增长试验是可靠性增长活动的主要内容，是产品工程研制阶段单独安排的可靠性工作项目，成为工程研制阶段的组成部分。

值得注意的是，尽管可靠性增长试验与环境应力筛选同为装备研制生产的可靠性工程试验，它们的目标都是为了暴露产品缺陷，但两者在具体任务上有明显区别，前者旨在暴露某些设计缺陷，纠正后可提高产品固有可靠性水平；后者旨在暴露工艺和元器件、原材料的缺陷，消除产品潜在的早期失效，并非为了提高产品的固有可靠性水平。

6.5.2 可靠性增长试验的时机

可靠性增长试验通常安排在工程研制基本完成之后和可靠性鉴定试验之前进行。此时，产品的性能与功能已经基本达到设计要求，产品结构与布局已经接近批生产的要求，故障信息的确实性已经较高，且此时故障纠正措施的实施所需资源和时间较少。使用阶段的可靠性增长活动可以利用产品的现场故障信息和现场使用状况记录来取代可靠性增长试验工作。

6.5.3 可靠性增长试验方法

一般来说，一个产品研制基本完成后，其可靠性一般只能达到其成熟阶段水平的 10% 左右，其内部隐藏着大量的故障隐患，包括配套元器件的质量、设计上的失误、不成熟的制造工艺，以及生产管理上的差错造成的问题等，必须在产品鉴定前加以解决。国内外资料统计表明：要使产品达到预期的可靠性水平，一般需要投入 5~25 倍 MTBF 目标值的可靠性增长试验时间，因此，必须要有相当的人力、物力和经费投入，并应科学、合理地做好计划安排，应在有关部门的共同配合下开展。

可靠性增长试验的一般方法是采用：“试验—分析—纠正—再试验（即 TAAF）”的工作模式，其基本工作步骤如下。

1. 制订试验计划

在开展可靠性增长试验工作前，首先要了解产品当前的可靠性水平（可根据现场使用情况，或可靠性摸底试验和产品环境应力筛选的结果推断），以及产品预期要达到的可靠性目标，由此根据可投入的资源，包括样品、试验设备、试验经费和时间、人力等，制订出工作计划，以计划增长曲线为基准，选用合适的可靠性增长模型开展试验。

制订可靠性增长计划的原则是，围绕可靠性增长曲线安排工作内容、进度、资

源、经费等。

确定产品可靠性增长曲线的方法是，根据同类产品研制所得的数据，经过分析，建立可靠性增长模型，确定其可靠性增长试验的时间长度；同时根据产品的可靠性指标，作为点估计值拟定可靠性增长曲线；据此安排试验项目、时间起点、预定的可靠性增长率等。

可靠性增长计划的主要内容包括：

- 试验的目的和要求。
- 受试产品及其应进行的试验项目。
- 试验剖面、产品技术状况、性能和循环工作周期。
- 试验进度安排。
- 试验设备、装置的说明及要求。
- 用于改进设计所需要的资源和时间要求。
- 试验数据的收集和记录要求。
- 故障报告、分析和纠正措施。
- 试验结果和产品的最后处理。
- 其他有关事项。

其中，应特别注意确定试验剖面。可靠性增长试验的目的是暴露产品在使用状态下的问题和缺陷，因此试验剖面要模拟实际的使用环境条件。实际使用环境条件又称任务剖面。对某些产品来说，可能有多种任务剖面，此时可取其中有代表性的典型任务剖面作为可靠性增长试验的试验剖面。如果选择不典型任务剖面，则选取环境条件最恶劣的任务剖面作为可靠性增长试验剖面，这样最有利于暴露设计缺陷。

2. 可靠性增长试验

试验以诱发产品在实际使用条件下可能发生的故障隐患为目的，科学、合理地选择试验条件和试验项目。目前常用于产品可靠性增长的试验手段是采用温度+湿度+振动的综合环境试验，它可以有效地激发产品在实际使用中暴露出的大部分故障模式，并已被国内外大量试验范例所证实。当然可靠性增长试验也可以结合其他类型的试验一起进行。

无论在何种状况下进行可靠性增长试验，都必须对试验的全过程进行详细记录，需要记录样品的技术状况和故障表现。这些资料是分析和判定设计缺陷、提出纠正措施的基本依据。记录的内容可参考有关标准导则所附的表格，以便统一可靠性增长试验、可靠性增长管理及可靠性信息系统所用的表格。

3. 故障分析与改进

必须对试验中暴露出来的产品故障开展故障定位与故障机理的分析。产品可靠

性增长的内涵是要提高产品固有的可靠性水平，而要提高其固有可靠性的关键是要找出存在于产品中的共有的故障隐患，或称系统性故障，只要当这些系统性故障被发现、被纠正后，产品固有的可靠性才能得到提高。如果在可靠性增长试验中被迫发现和纠正的，仅仅是个别的偶然性故障，或称残余性故障，那是不充分的，因此必须对试验中发现的故障进行认真分析，找出系统性故障，并采取措施加以纠正。对于系统性故障的纠正，只能通过修改产品设计或改进生产工艺等途径实现。单纯的故障修复或更换措施，只能用于排解残余性偶发故障，而无助于产品固有可靠性的提高。

4. 再试验

经过改进的产品，仍需开展进一步的试验：一是为验证改进措施的有效性；二是继续暴露产品尚存的故障隐患，开展进一步的可靠性增长，直至达到预定的可靠性目标为止。

6.5.4 常用可靠性增长模型

目前，在可修产品的可靠性增长试验中，普遍使用的是杜安（Duane）模型。有时，为使杜安模型的适合性和最终评估结果具有较坚实的统计学依据，可用AMSAA模型作为补充。

1. 杜安模型

杜安模型最初是飞机发动机和液压机械装置等复杂可修产品可靠性改进过程的经验总结。模型未涉及随机现象，所以杜安模型是确定性模型，即工程模型，而不是数理统计模型。

杜安模型的前提是：产品在可靠性增长过程中，逐步纠正故障，因而产品可靠性是逐步提高的，不允许有多个故障集中改进而使产品可靠性有突然的、较大幅度的提高。

设可靠性增长试验的开始时刻为 $t=0$ ， t 为试验过程中某个时刻的累积试验时间， $r(t)$ 为试验时间段 $(0,t)$ 内受试产品发生的关联故障数。

关联故障数 $r(t)$ 实际上是一个非连续函数，因为故障计数只能是非负整数。杜安模型在其规定的前提下，把 $r(t)$ 当成连续函数来处理。

杜安模型引入累积故障率概念，用 $\lambda_{\Sigma}(t)$ 表示，其定义为

$$\lambda_{\Sigma}(t) = \frac{r(t)}{t} \quad (6-18)$$

注意，这里的累积故障率与电子产品中的故障率 $\lambda(t)$ （即瞬间故障率）是两个

不同的概念。

累积故障率是一个计算值，没有具体的物理意义，但是累积故障率在随着累积试验时间 t 增加时的变化规律中蕴含着产品可靠性变化规律。

杜安通过分析发现，产品在增长试验过程中，累积故障率对于累积试验时间而言，在双边对数坐标纸上趋近于一条直线，即：

$$\begin{aligned}\ln \lambda_{\Sigma}(t) &= \ln \left(\frac{r(t)}{t} \right) \\ &= \ln a - m \ln t\end{aligned}\quad (6-19)$$

或

$$\lambda_{\Sigma}(t) = \frac{r(t)}{t} = at^{-m} \quad (6-20)$$

式中，参数 a 与 m 分别是双边对数坐标纸上该直线的截距（ $t=1$ 时的确切截距是 $\ln a$ ）和斜率（确切的斜率为 $-m$ ）。

由此可得出关联故障数的数学式：

$$r(t) = at^{1-m} \quad (6-21)$$

对于可修产品，在可靠性增长过程中某一时刻产品具有的可靠性水平，杜安模型用故障强度度量 $\lambda(t)$ 表示：

$$\lambda(t) = \frac{d}{dt} r(t) \quad (6-22)$$

$$\lambda(t) = a(1-m)t^{-m} \quad (6-23)$$

由于当前可修产品的可靠性参数常用 MTBF，因此在运用杜安模型时，派生出两个术语：累积 MTBF，用 $MTBF_{\Sigma}(t)$ 表示；瞬时 MTBF，用 $MTBF(t)$ 表示。在故障间隔时间序列服从指数分布的假设下，这两个 MTBF 与相应故障率成互为倒数关系，由此可得出这两个 MTBF 的数学式：

$$MTBF_{\Sigma}(t) = \frac{1}{a} t^m \quad (6-24)$$

$$MTBF(t) = \frac{1}{a(1-m)} t^m \quad (6-25)$$

这两个 MTBF 式是杜安模型的主要结论之一，当参数 a 与 m 确定后，它表述了产品可靠性在可靠性增长试验中的变化规律。

杜安模型的另一个主要结论是由式（6-24）、式（6-25）导出的累积 MTBF 与瞬时 MTBF 的关系式：

$$MTBF(t) = \frac{MTBF_{\Sigma}(t)}{1-m} \quad (6-26)$$

两边取对数，则有：

$$\ln \text{MTBF}(t) = \ln \text{MTBF}_{\Sigma}(t) + \ln \frac{1}{1-m} \quad (6-27)$$

式(6-26)表明在可靠性增长试验过程中任一时刻产品的瞬时 MTBF 是累积 MTBF 的 $1/(1-m)$ 倍; 式(6-27)表明, 在双边对数坐标纸上, 在任一时刻, 瞬时 MTBF 总是高于累积 MTBF, 高出量为常数值: $-\ln(1-m)$ (在可靠性确实增长的情况下, m 值为 0.5 左右)。由于累积 MTBF 在可靠性增长试验中很容易计算出来, 利用式(6-26)、式(6-27)就可求得产品在增长过程中的瞬时 MTBF, 这使得杜安模型应用非常方便。

杜安模型在双边对数坐标纸上和线性坐标纸上的形状如图 6-11 所示。

参数 m 称为杜安增长率, 在不会引起误解时可简称为增长率。由于对于一个特定产品, 在杜安模型适用条件下, 增长率 m 为一常值, 这容易误解成在可靠性增长试验过程中, 产品的 MTBF 是线性增长的。实际上, 在杜安模型下, 产品 MTBF 对于试验时间, 其增长是先快后慢, 如图 6-11 (b) 所示。

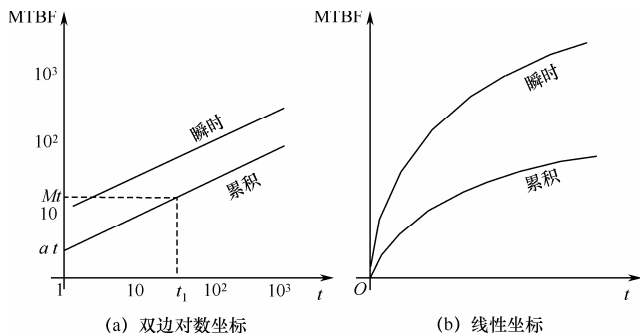


图 6-11 杜安模型形状

在 TAAF 试验中, 前期诱发的故障通常是故障率较高的故障, 通过纠正后产品的 MTBF 将有较大的提高。而在后期诱发的故障则正好相反, 此时, 通过纠正后产品 MTBF 的提高量相对比较少一些。杜安模型恰好总结了这个规律。

参数 a 的几何意义是: 它的倒数是杜安模型累积 MTBF 曲线在双边对数坐标纸上当累积试验时间 $t=1$ 时的截距。参数 a 的物理意义是: 它的倒数在一定意义上反映了产品进入可靠性增长试验时的 MTBF 水平。参数 a 决定于产品在增长试验前研制工作中可靠性设计的效果。其所以说“在一定意义上反映”, 是因为对应的累积试验时间 t 不为零, 而且 t_l 和 M_l 替代 a , 即将如下公式:

$$a = \frac{1}{M_l} t_l^m \quad (6-28)$$

代入式(6-24)、式(6-25)得出:

$$\text{MTBF}_{\Sigma}(t) = M_l \left(\frac{t}{t_l} \right)^m \quad (6-29)$$



$$\text{MTBF}_{\Sigma}(t) = \frac{M_l}{1-m} \left(\frac{t}{t_l} \right)^m \quad (6-30)$$

式(6-29)、式(6-30)是杜安模型中两个重要的应用公式。式(6-30)用于制订增长计划,式(6-29)用于表示增长计划曲线并用于跟踪,两者还用于产品可靠性增长过程中及最终的可靠性评估。

从理论上讲,杜安模型有明显的不足之处。由式(6-25)可以看到,在杜安模型下,当 $t \rightarrow 0$ 时,产品的瞬时 MTBF 趋于零。这是模型虚构的情况,实际产品的瞬时 MTBF 不可能为零。又当 $t \rightarrow \infty$ 时,产品瞬时 MTBF 增大到无穷大,这说明产品的瞬时 MTBF 可以无限制地增长。这也是不可能的。但是实践表明,杜安模型在这两点理论上的不足,不影响其在可靠性增长试验中的应用。

杜安模型形式简单,模型参数的物理意义容易理解,便于制订增长计划,增长过程跟踪简便,用工程方法可方便地对最终结果给出评估,所以,杜安模型在可靠性增长试验中得到广泛应用。杜安模型的主要不足是模型中未考虑随机现象,因而对最终结果不能提供依据数理统计的评估。

2. AMSAA 模型

AMSAA 模型是杜安模型的改进型,具体的模型、方法和算例请参见 GJB 1407-1992 附录 B。

6.5.5 可靠性增长试验计划曲线

可靠性增长试验计划的主要组成部分是计划曲线,制订计划曲线要依据所选的增长模型。本节介绍以杜安模型制订计划曲线的方法,以及有关计划的一些其他问题。

1. 计划曲线

杜安模型描述产品可靠性在增长试验过程中的增长规律时有两种形式,如式(6-29)、式(6-30)所示,分别以累积 MTBF 与瞬时 MTBF 为因变量。

计划曲线采用以累积 MTBF 为因变量的形式,即式(6-29)的形式。其原因是这种形式便于后续跟踪。跟踪是记录产品可靠性的实际增长过程,以便在与计划曲线对比的基础上对实际增长过程实施控制。在跟踪过程中累积 MTBF 很容易计算,而且与实际增长过程的模型参数无关。而瞬时 MTBF 计算必须要用到实际增长过程的增长率 m 估计值。随着试验的推进,故障数据的增加, m 的估计值是不断变动的。那么每一次 m 估计值的变动将导致对这之前的所有瞬时 MTBF 计算值的修改,所以是极其繁杂的。

计划曲线的数学式,即式(6-29)中仅有 3 个参数: M_l 、 t_l 和 m ,但是不能随意地选定这 3 个参数。可靠性增长试验是有目标计划的可靠性增长,要求在消耗完

给定资源（以总试验时间为代表）时，产品可靠性应达到或超过增长目标。

设 T 为总试验时间， M_{obj} 为预期的增长目标（要注意 M_{obj} 是瞬时 MTBF），那么根据式（6-30），下列关系式必须满足：

$$M_{obj} \geq \text{MTBF}(T) = \frac{M_I}{1-m} \left(\frac{T}{t_I} \right)^m \quad (6-31)$$

式中共有 5 个参数，它们是 M_I 、 t_I 、 m 、 T 、 M_{obj} 。只有当这 5 个参数满足上述关系时，将其中的 M_I 、 t_I 、 m 代入式（6-29）才能构成符合增长试验目的的计划曲线。

下面分别介绍如何确定各个参数。

（1）增长目标的确定

通常增长目标 M_{obj} 是由合同任务书规定的。

如果合同任务书中未做规定，而有已经确定了的可靠性鉴定试验的试验统计方案，那么可选取能使产品以高概率通过可靠性鉴定试验的 MTBF 值作为增长目标。高概率应不小于 0.8。

当用上述两种方法确定增长目标后，在条件许可时，应当用最新可靠性预计和可靠性增长潜力作为增长目标是否合适的补充说明。

（2）起始点的确定

计划曲线的起始点包含两个参数： M_I 、 t_I 。

由于起始点 M_I 和 t_I 蕴含着杜安模型的参数 a 和 m ，它们对增长规律、总试验时间有很大影响。

确定起始点的最好方法是总结上代产品或同类产品的增长规律。

有的资料中提供了确定 M_I 、 t_I 的一般原则：

$$\left. \begin{aligned} M_I &= 0.1 \sim 0.3 M_{obj} \\ \text{当 } M_{obj} &\geq 200\text{h, 则 } t_I = 0.5 M_{obj} \\ \text{当 } M_{obj} &< 200\text{h, 则 } t_I = 100\text{h} \end{aligned} \right\} \quad (6-32)$$

式中的 M_{obj} 亦有用最新可靠性预计 M_p 替代的，但对这种选取方法，还有争议。

（3）杜安增长率的确定

最初，杜安模型依据的一些航空用履机和液压机械装置的增长率都是 0.5。随后，经过比较广泛的可靠性增长试验的实践，对于新研制的复杂设备，增长率的范围为 0.3~0.6。

（4）总试验时间的确定

由于可靠性增长试验既要诱发产品故障，又要验证故障纠正措施的有效性，所

以没有足够的总试验时间 T ，是不能达到预期目的的。再者，总试验时间直接关系到可靠性增长试验所需消耗的资源，资源短缺使得人们对尽可能减少总试验时间格外关心，这是一个矛盾。

工程实践表明，总试验时间 T 可取为增长目标 M_{obj} 的 5~25 倍。对于高可靠性目标的产品，因经费的限制，可以取低值。

借助较高的增长率，即加大故障纠正力度有助于适当减少总试验时间。但是，过低的总试验时间，将会加大可靠性增长试验达不到预期增长目标的风险。

(5) 制订计划曲线的有关公式

以上介绍了 5 个参数的确定原则与数值范围，但在实际制订计划曲线时不是简单地确定 5 个参数就能完成的。

首先，这 5 个参数是相互制约的。其次，在制订计划曲线时不能过分强调达到预期增长目标的必要性，而忽视了总试验时间、增长率以及计划曲线起始点实现的可能性。忽视这些可能性将会导致可靠性增长试验的失败，预期增长目标也将不能达到。

所以，制订计划曲线是反复权衡的过程，要不断地反复计算 5 个参数，不断地修改，最后才能得出比较满意的计划曲线。

$$M_{obj} = \frac{M_I}{1-m} \left(\frac{T}{t_I} \right)^m \quad (6-33)$$

$$M_I = (1-m) \left(\frac{t_I}{T} \right)^m M_{obj} \quad (6-34)$$

$$t_I = T \left[\frac{M_I}{(1-m)M_{obj}} \right]^{1/m} \quad (6-35)$$

$$m \approx -1 - \ln \left(\frac{T}{t_I} \right) + \left\{ \left[1 + \ln \left(\frac{T}{t_I} \right) \right]^2 + 2 \ln \left(\frac{M_{obj}}{M_I} \right) \right\}^{1/2} \quad (6-36)$$

$$T = t_I \left[\frac{(1-m)M_{obj}}{M_I} \right]^{1/m} \quad (6-37)$$

2. 制订计划曲线举例

【例 6-7】可靠性增长计划

某产品的增长目标，依据以 0.9 的概率通过可靠性鉴定试验，确定为 $M_{obj}=62h$ 。

根据产品设计的成熟程度、承制方技术与管理水平，初步确定增长率 $m=0.4$ 。

初步制订了增长策略，确定纠正比 $K_\lambda=0.9$ ，平均纠正有效性系数 $d=0.7$ 。利用式 (6-34) 求出 $M_I=11.5h$ 。根据同类产品实际可靠性增长规律，增长过程趋于稳

定时, M_I 约为 12.5h, 相应 t_I 约为 80h。综合两方面的情况, 初步确定 $M_I=12\text{h}$ 、 $t_I=80\text{h}$ 。

由式 (6-37) 算出共需总试验时间 $T=1354\text{h}$ 。经可用资源分析, 嫌 T 略多了些, 准备限制在 1200h。

把总试验时间限定在 1200h, 由式 (6-36) 算一下增长率将增大到多少。计算后的结果 $m \approx 0.42$ 。经分析, 认为 $m \approx 0.42$ 可以接受。

最后得出计划曲线中的各参数: $M_I=12\text{h}$, $t_I=80\text{h}$, $m=0.41$, $T=1200\text{h}$, $M_{obj}=62\text{h}$ 。

6.5.6 可靠性增长试验的跟踪与控制

1. 跟踪与跟踪曲线

跟踪实际增长过程的具体做法是:

① 准备一张双边对数坐标纸。把以累积 MTBF 为因变量的计划曲线画在坐标纸上, 从横坐标 t_I 处画到 T 处。在 t_I 的左边要留一级对数坐标量的空白, 以便跟踪 $[0, t_I]$ 期间的增长过程。为便于监控, 可用虚线把计划曲线延伸到小于 t_I 的区域中。

② 在可靠性增长试验过程中, 每当发生一次关联故障, 应记下故障时间 t_i 和当时的累积故障数 $r(t_i)$, 并用下式计算当时的累积 MTBF, 用简化符号 M_i 表示:

$$M_i = \text{MTBF}_{\Sigma}(t_i) = \frac{t_i}{r(t_i)} \quad i=1, 2, \dots, n \quad (6-38)$$

③ 把每一个关键故障对应的点, 画到双边对数坐标纸上, 其坐标为 (t_i, M_i) 。

随着故障次数的增加, 逐渐形成一张跟踪点图。跟踪点图的形状如图 6-12 所示。跟踪过程有时需要绘制跟踪曲线。

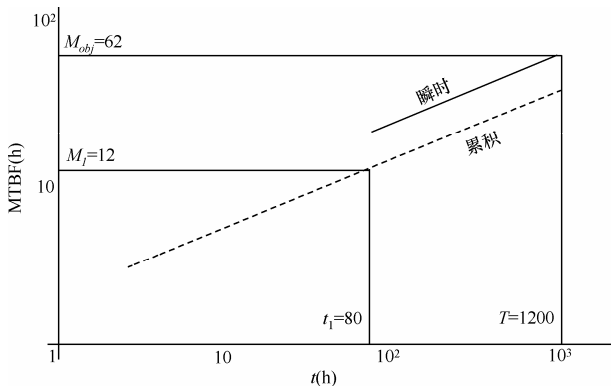


图 6-12 增长过程的跟踪



2. 控制与决策

根据跟踪情况，在与计划曲线进行对比后，在必要时可对实际增长过程实施控制。实际增长过程符合下列三种情况之一时，可判定为满意，无需进行控制：

- 所有故障点都在计划曲线上或上方。
- 跟踪曲线在计划曲线上或上方。
- 跟踪曲线向右方（未来时刻）延伸后将在总试验时间 T 之前穿过计划曲线。

如果实际增长过程不符合上述三种情况中的任一种时，可靠性增长试验失败的可能性很大，因此要采取措施以控制实际增长过程的增长率。

主要措施是改善增长策略提高故障纠正效果，即：

- 提高纠正比，重新审定故障分类，进行费效比权衡，把一些未纠正的故障纠正。
- 提高故障纠正的有效性，为此要加强故障分析提高分析准确性，找准故障原因和故障机理，并采取强有力的纠正措施。

如果在采取强有力的措施后，实际增长过程仍不能满意，其原因可能是增长率过大过于冒进，或是受试产品初始可靠性失控，远未符合计划曲线的要求，这时需要采取重大决策。决策之一是调用备用资源或申请追加资源以增加总试验时间。如果这样做了后预计仍不能达到预期增长目标，此时只能采取果断决策，中止试验，进行专题研究。

如果在增长试验过程中，很少出现关联故障，甚至不出现关联故障，这时首先要仔细审查试验方法是否有问题，故障是否有漏检等。当排除了这些原因时，那么可以提前结束试验，按可靠性鉴定试验的评估方法对产品可靠性做出评估。

6.5.7 可靠性增长试验的最终评定

当累积试验时间达到计划的 T 时，可靠性增长试验结束，此时，跟踪过程提供了全部故障时间序列，通常是时间截尾数据，可以以此对可靠性增长试验做出评定。

6.6 加速试验

6.6.1 加速试验的目的和基本原理

1. 加速试验的目的

前几节介绍的几种常规可靠性试验方法虽然非常有用，但试验时间通常较长，

特别是对可靠性水平高的产品更是如此。为了实现缩短产品上市周期、降低产品成本的目标，满足人们对经济高效加速试验方法的需求，这些加速试验方法是通过提高产品试验的应力水平或者增大交变应力施加的频度而缩短试验时间，并发现和减少产品的失效模式，以便快速评估产品的可靠性水平，使其得到增长。

加速试验的目的主要有：

- 快速暴露产品的设计和制造缺陷，并采取有效的纠正措施，提高产品的应力裕度，增强产品的健壮性。
- 通过试验室加大应力的加速试验，快速验证产品的外场使用可靠性。
- 消除产品的早期失效。

加速试验一般可分为定性和定量两种形式。定性加速试验的目的是发现最终可能导致产品现场使用失效的潜在故障；定量加速试验则是根据加速模拟试验结果来评估产品可靠性。加速模拟试验条件是以产品使用环境和使用剖面为基础确定的。

2. 加速试验的基本原理

任何类型的加速试验都基于加速损伤理论。产品在其寿命周期内所经历的应力可对其造成渐进的累积损伤。这种损伤有时可能造成产品使用（外场）失效，但有时也不会造成其使用失效。

任何类型加速试验的方法原理，都是通过提高试验应力来产生与产品寿命期内预期应力产生相同的累积损伤。产品破坏应力极限的确定为评估破坏应力极限与产品规范规定的应力极限之间是否有足够的余量提供信息，因此，该试验方法可为产品在其寿命期内不发生与相关应力类型有关的失效提供保证。加速试验主要不是定量确定产品寿命概率分布，而是对产品的应力强度进行必要的调整，以避免此类故障在产品使用过程中的发生。这种确定产品足够的应力余量与其寿命概率分布无关的试验是一种定性试验。确定产品寿命概率的试验，试验中的应力量值与产品在超过其预期寿命内应力量值的寿命概率有关，这种试验类型则是定量的。

图 6-13 描述了定性与定量加速试验的累积损伤原理。为了方便起见，所有的应力（工作应力极限、破坏应力极限等）都用绝对值表示。产品技术规范规定的应力值通常给出上、下两个极限值，因此，有技术规范规定的上限及下限（USL 和 LSL），同样也有设计上限和下限、工作应力上限和下限、可靠性试验上限和下限。从基本原理上讲，负应力也可能以不同的故障机理对产品产生累积损伤，因此对于在负应力作用下产品规定限值与预期限值之间关系的描述方式，可参考产品在正应力作用下的描述方式。例如，低温极限可能对产品产生与高温极限相同的失效模式。为了避免混乱，在图 6-13 中不区分正温度应力、负温度应力或者其他正负应力，因此，应力量值无论正负，都用上限或者下限的绝对值表示。

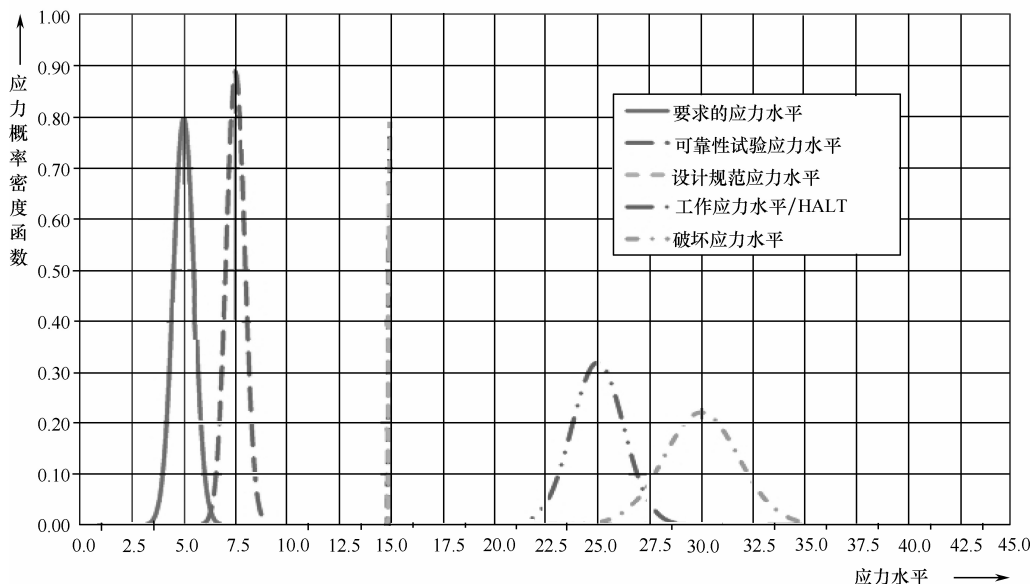


图 6-13 累积损伤、退化的概率密度函数及试验类型

图 6-13 中的曲线表示了在产品全寿命周期内（从寿命开始时刻 t_0 到寿命终结 t_L ）对应于某一应力的要求强度。试验中的产品强度和应力假设服从高斯分布。

图 6-13 描述了加速试验的不同类型。功能性试验是在产品需求说明书规定的范围内的某一个应力水平下开展的。在这个应力条件下，要求产品在整个试验过程中不能发生故障。产品的设计需要验证以确保其在技术规范规定的上下应力极限内可正常工作。例如，加速退化试验或累计损伤试验可获取产品设计规范规定的应力水平与可靠性验证试验应力水平之间的间隔余量。当产品的性能指标退化超出其需求说明书所规定的值且这种状态定义为失效时，产品判定为不合格。当在 t_0 时刻对产品进行测试时，对于产品承受的应力值小于或等于设计规范规定的应力水平的情况，其不应发生任何失效。

产品设计规范应考虑因其寿命周期内所经受的应力累积损伤而引起的某些性能退化。为了提供必要的应力余量，产品设计规范规定的应力极限应大于产品使用过程中要求的应力极限。当预期应力累积损伤导致产品性能退化后，可靠性试验提供了试验应力水平（剩余强度）与要求的应力水平之间的应力余量信息。这个余量值就是在规定的时间 t_L 内的可靠性水平值。

产品设计极限强度比设计规范规定的强度高得多，该极限强度由以寻找产品设计的薄弱环节为目的的定性加速试验来确定。在产品寿命期内，随着性能退化，其设计薄弱环节可能会影响可靠性指标，因此，在产品工作应力极限（OL）下开展定

性加速试验来验证产品的强度。

产品的破坏应力极限 (DL) 大于产品的工作应力极限。在破坏应力极限作用下产品将发生永久性失效。如果产品的工作应力极限 (或破坏应力极限) 与其设计规范规定的应力极限接近, 产品的工作应力极限或破坏应力极限分布的标准偏差大时, 则定性加速试验就可以暴露产品设计的潜在薄弱环节。

产品的可靠性是时间的函数, 一般情况下定义为寿命时间 t_L 的函数。

产品使用要求的强度与可靠性试验应力水平之间余量 (应力均值之差除以它们的标准差) 的累积正态分布体现了产品的可靠性。试验应力水平及其持续时间的选择, 应考虑试验产生的累积损伤与产品寿命周期内因累积损伤而引起的性能退化效果相一致。确定产品要求的可靠性水平的计算值即是定量评价价值。

下面介绍几种典型的加速试验。

6.6.2 加速寿命试验

1. 加速寿命试验的分类

加速寿命试验按施加应力的方法大致分为三种类型: 恒定应力加速寿命试验; 步进应力加速寿命试验、序进应力加速寿命试验。

将投试产品分成 n 组, 每组在高于正常应力水平的恒定不变的应力下进行的试验称为恒定应力加速寿命试验; 每组的应力不仅高于正常水平而且随时间分阶段逐步增强的试验称为步进应力加速寿命试验, 如图 6-14 (a) 所示。如果所加的应力是随时间等速增加, 那么称为序进应力加速寿命试验, 如图 6-14 (b) 所示。无论是哪一种应力, 它都必须在一定的强度范围内, 力求保证以下 3 点: (1) 失效机理的不变性; (2) 存在有规律的加速过程; (3) 退化或失效的分布模型应具有统一性或规律性。

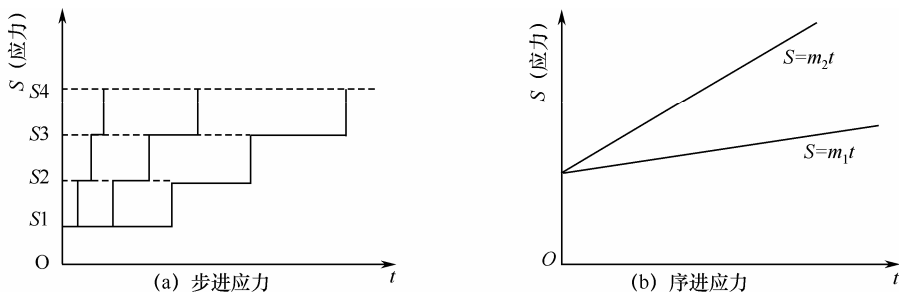


图 6-14 步进应力和序进应力的加速寿命试验

施加高应力后的试验如果能达到这三点, 就是理想的加速寿命试验。在理想情

况下，高应力水平作用下的产品退化方式与正常应力水平下的相同，只是时间缩短罢了，那么一个小时高应力水平的试验能产生与 t 小时正常应力水平试验完全相同的效果。但实际上理想的加速寿命试验是做不到的。尽管如此，加速寿命试验的结果仍有很大的参考价值。这种试验可以大大缩短试验周期，节省投试产品和试验费用。但由于产品在高应力下的退化方式可能与正常应力不同，而使预测的准确度降低。相对而言，上述提到的 3 种试验中恒定应力加速寿命试验造成失效的因素较单一，准确度较高，试验容易取得成功，只是试验周期长些。下面主要介绍这种试验方法的基本原理和加速倍数的计算。

2. 加速寿命试验的原理和加速模型

恒定应力加速寿命试验的原理就是产品的寿命与所加应力的大小有关，应力越大，产品的寿命越短。

如图 6-15 所示，对某一产品施加 5 种高于正常水平应力的恒定应力 S_i 就得到 5 种不同的寿命数据 t_i ，将图示加速寿命曲线延长，A 点对应的应力 S_0 为正常应力， t_0 为正常应力水平下产品寿命之预测值。

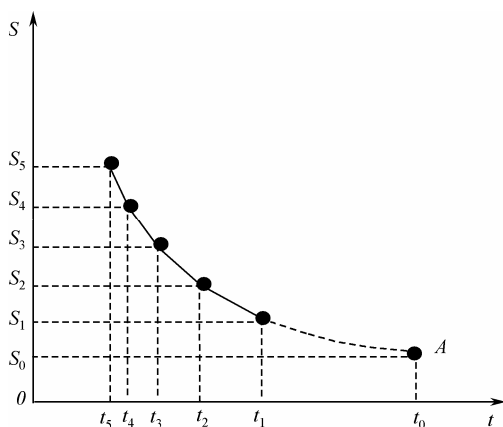


图 6-15 加速寿命曲线示意图

在温度恒定应力加速寿命试验中，常采用阿列尼斯方程作为寿命与温度关系的模型。阿列尼斯方程是表示化学反应与温度关系的一个经验公式，即：

$$\frac{dM}{dt} = A \exp\left(-\frac{E}{kT}\right) \quad (6-39)$$

式中， M 为化学反应量； A 为比例常数； T 为绝对温度 (K)； k 为玻尔兹曼常数 ($0.8617 \times 10^{-4} \text{ eV/度}$)； E 为激活能 (单位：eV)。

若元器件的失效是由某种反应量的原始值 M_0 累积到一定程度 M 所引起的，那

么其寿命就是反应累积到 M 所需的时间 t ，由阿列尼斯方程两边积分可得到：

$$t = \frac{M - M_o}{A} e^{\frac{E}{kT}}$$

两边取对数可得到：

$$\ln t = \ln \frac{M - M_o}{A} + \frac{E}{k} \cdot \frac{1}{T} \quad (6-40)$$

或

$$\lg t = \lg \frac{M - M_o}{A} + \frac{Elge}{k} \cdot \frac{1}{T} \quad (6-41)$$

设： $a = \lg \frac{M - M_o}{A}$ 、 $b = \frac{E}{k}$ ， 或 $a' = \lg \frac{M - M_o}{a}$ 、 $b' = \frac{Elge}{k}$ ， 寿命 θ 用 t 表示， 则有 $\ln t = a + b \frac{1}{T}$ 或 $\lg t = a' + b' \frac{1}{T}$ ， 即寿命的对数与绝对温度的倒数之间满足直线方程。

因此，通过几个不同温度点的试验得到元器件在这几个温度点的寿命后，就可以估计出上式中的几个常数，并利用这一关系外推出正常温度下的元器件寿命和表征元器件失效机理的激活能 E 。

在电压恒定应力加速寿命试验中，常采用逆幂律作为寿命与电应力关系的模型，即：

$$t = \frac{1}{KV^a} \quad (6-42)$$

式中， V 为施加电应力； K 、 α 为常数，其中 α 称为材料结构常数，只与元器件的类型有关，而与其规格无关。对于符合上述关系的元器件，则其寿命的对数与所施加电压的对数之间满足直线方程：

$$\ln t = -\ln K - a \ln V \quad (6-43)$$

或

$$\lg t = \lg K - a \lg V \quad (6-44)$$

设： $A = -\ln K$ 或 $A = -\lg K$ ， $B = -a$ ， 则有： $\ln t = A + B \ln V$ 或 $\lg t = A + B \lg V$ ， 因此，通过几个不同电应力点的试验得到元器件的不同寿命后，就可以估计出上式的几个常数，并利用这一关系式外推出正常负荷下的元器件寿命。

恒定应力加速寿命试验一般选取 4~5 个应力水平进行试验。最高应力在不改变元器件失效机理的前提下，尽量选得高一些，以期达到最大的加速效果，但不得高于产品的结构、材料以及制造工艺所能承受的应力极限。最低应力在保证加速效果的前提下，尽量接近实际应力水平，以期提高外推的准确性。每一应力水平下的试验样品数量，视产品的情况及试验能力而定，一般在 25~100 的范围内。

在基准应力条件下进行的试验与在某种应力条件下的加速试验，两者达到相等的累积失效概率所需要时间的比值称为加速因子或加速系数，通常用符号 AF 表示。例如，在基准应力条件下元器件工作到 1000 小时累积失效概率达到 50%，而在加速试验中，元器件工作到 10 小时累积失效概率就达到 50%，则 $AF=1000 / 10=100$ 。

加速寿命试验的失效模型有以下几种。

(1) 阿伦尼斯 (Arrhenius) 方程

1899 年阿伦尼斯根据试验结果总结出化学反应率与温度间关系的经验公式，将寿命 θ 用 t 表示，重写式 (6-40) 可得：

$$\ln t = a + b \left(\frac{1}{T} \right) \quad (6-45)$$

式中， t 为产品的寿命； T 为加速应力（温度）。

式 (6-45) 就是由阿伦尼斯方程导出的加速寿命方程，它给出了产品寿命 t 与加速应力（温度 T ）之间的关系，与之对应的曲线便是加速寿命曲线。显然，在单对数坐标系上，式 (6-45) 表示 t 与 $\frac{1}{T}$ 是一条直线关系。反之，如果根据某产品的加速寿命试验数据，在单边对数坐标纸上描点，所得的轨迹可用直线拟合，那么该产品的寿命与温度满足关系式 (6-45)。更进一步，在拟合直线延长线上可以得到正常应力（温度）水平下的寿命数据。

加速系数如下：

$$AF = \exp\left(-\frac{E}{k}\right)\left(\frac{1}{T_S} - \frac{1}{T_0}\right) \quad (6-46)$$

式中， T_S 加速温度， T_0 是正常温度。

(2) 逆幂律方程

有些产品的寿命 t 与所加电压 U 、所通电流 I 之间符合逆幂律关系，分别重写式 (6-43)，则有：

$$\lg t = -C \lg U - \lg K_U \quad (\text{电压}) \quad (6-47)$$

$$\lg t = -C \lg I - \lg K_I \quad (\text{电压}) \quad (6-48)$$

式中， K_U 、 K_I 、 C 均为常数。

如果产品寿命 t 与所加电压或电流之间满足式 (6-47) 或式 (6-48)，则可在双对数坐标系上获得加速寿命直线。

加速系数如下：

$$AF = \left(\frac{V_S}{V_0} \right)^\alpha \quad (6-49)$$

式中, V_S 加速电应力; V_0 是正常电应力。

(3) 温度与电应力作为加速应力

如果以温度和电应力同时作为加速应力, 对于电容器可采用的加速寿命方程为

$$t = \frac{A}{U^C} \exp\left(\frac{B}{T}\right) \quad (6-50)$$

式中, U 为电应力; T 为绝对温度; A 、 B 、 C 都是参数。

加速系数为

$$AF = \left(\frac{V_S}{V_0}\right)^\alpha \exp\left(-\frac{E}{k}\right)\left(\frac{1}{T_S} - \frac{1}{T_0}\right) \quad (6-51)$$

(4) 温度、相对湿度作为加速应力

如果用温度、相对湿度同时作为加速应力, 可采用的加速寿命方程为

$$t = B \exp\left(\frac{E}{kT}\right) \exp[-(RH^n)] \quad (6-52)$$

加速系数如下:

$$AF = \exp\left\{\left(\frac{E}{k}\right) \cdot \left[\left(\frac{1}{T_0}\right) - \left(\frac{1}{T_s}\right)\right] + (RH_0^n - RH_s^n)\right\} \quad (6-53)$$

式中, E 为激活能 (eV); k 为玻尔兹曼常数且 $k=8.6 \times 10^{-5}$ eV/K, T 为绝对温度, RH 是指相对湿度 (%), 下标 0 表示常态, 下标 s 表示加速状态; n 为常数, 一般取 2~3。

(5) 温度与电应力作为加速应力

如果以温度和电应力同时作为加速应力, 对于微电路可采用的艾森方程为

$$t = \frac{G}{T} \exp\left[\frac{E}{kT} - U\left(C + \frac{D}{kT}\right)\right] \quad (6-54)$$

式中, G 、 C 、 D 为常数; E 为激活能; k 为波兹曼常数; T 为绝对温度; U 为偏压。

【例 6-8】加速试验的指标测定计算

某计算机产品, 要求在 90% 的置信度下 MTBF 为 20000h, 因单价较贵, 只能提供 10 台左右的产品做试验, 请问如何判定此产品的可靠性是否达到规定的要求?

还是转化为求测试时间的问题。即使有 10 台产品全部用于测试, 20000h 的 MTBF 也需要每台试验 7780h 左右, 这个时间太长, 应该怎么办?

此时一般用到加速测试。对一般电子产品而言, 大多用高热加速, 有时也用高湿高热加速。可用式 (6-53) 计算加速因子, 由贝尔实验室资料可知 n 取 2。

激活能 E 根据原材料的不同, 有不同的取值, 根据相关文献, 一般可参考表 6-9。

表 6-9 不同失效模式的激活能

氧化膜破坏	0.3 eV
离子性	1.0~1.4 eV
按离子性	1.0eV
由于电迁移而断线	0.6eV
铝腐蚀	0.6~0.9eV
金属间化合物生长	0.5~0.7eV

根据产品的特性，由贝尔实验室资料可知 E_a 为 0.6eV ，试验加速应力设在 75°C 、 $85\%\text{RH}$ ，则在 75°C 、 $85\%\text{RH}$ 下做测试 1h ，相当于在室温（ 25°C 、 $75\%\text{RH}$ ）的加速倍数如下：

$$AF=\exp\{[0.6\times((1/298)-(1/348))\times8.6\times10^{-5}]+[0.85^2-0.75^2]\}=33.91$$

若允许一次失效，在 90%的置信度下，需要测试的时间为： $T_{test}=A*\text{MTBF}$ ，因此：

$$A=\frac{\chi^2_{(1-\alpha,2(r+1))}}{2}$$

式中， $\chi^2(1-\alpha,2(r+1))$ 是自由度为 $2(r+1)$ 的 χ^2 分布的 $1-\alpha$ 的分位数； $1-\alpha$ 是要求的置信度，在此例中为 90%； r 是允许的失效数，可自行确定。此分布值可以通过 Excel 来计算，在 Excel 中对应的函数为 Chiinv，如允许失效 1 次时：

$$A=0.5\times\text{CHIINV}(1-0.9, 2*2)=0.5*\text{CHIINV}(0.1, 4)=3.89$$

所以要求的室温下的测试时间： $T_u=3.89*20000=77800\text{h}$ ；换算后，在高温下的测试时间： $T_a=77800/AF=2294.31\text{h}$ ；最后，测试方案就是：将 10 台设备在 75°C 、 $85\%\text{RH}$ 下进行 229.43h 的测试，如果失效次数小于或等于 1 次，就认为此产品的 MTBF 达到了要求。

6.6.3 高加速极限试验和应力筛选试验

1. HALT/HASS 的内涵和主要作用

高加速极限试验（Highly Accelerated Limit Test，HALT）是指在规定的环境应力下，用于找出产品最有可能出现的失效模式的试验或试验序列。

HALT 的主要作用如下：

① 利用高环境应力，使产品设计缺陷显现出来，改善后大大提高设计可靠性，确保能获得早期高可靠性，使设备具有高的外场可靠性。

② 了解产品的设计能力及失效模式。

- ③ 作为高应力筛选及稽核规格制订的参考。
- ④ 快速找出产品研制中的瑕疵，大大减少鉴定试验时的故障。
- ⑤ 增加产品可靠度及减少维修成本。
- ⑥ 建立产品设计能力数据库，作为研发依据并可缩短设计制造时间。

高加速应力筛选（Highly Accelerated Stress Screening, HASS）是指为了激发出产品因制造工艺和控制差错而引入的潜在缺陷的试验。

HASS 的主要作用如下：

- ① 能用最低费用和最短时间激发出产品的潜在缺陷。
- ② 能用最低费用和最短时间检测出尽可能多的缺陷。
- ③ 提高产品外场可靠性。
- ④ 降低产品生产、筛选、维修和担保的总费用。

2. HALT 的主要原理

当可靠性鉴定试验或可靠性增长试验被加速时，需要证明试验应力所产生的累计损伤与产品寿命期内或产品可靠性验证的预定时期内所产生的累积损伤之间的余量。利用应力余量的好处就是可通过应力-强度准则得到产品在预定时间内的可靠性水平。产品的强度可通过试验结果得知，而可靠性水平就是以载荷-强度曲线交集以外的区域大小来表示（两条曲线的重叠区域代表发生失效），如图 6-16 所示。

为了估计设计规范与受试单元之间的应力余量，可通过增大试验应力直到产品发生失效的方式进行操作。这种高加速极限试验确定的余量可以以工作应力极限（OL）和破坏应力极限（DL）的方式给出。这也表明反映材料和生产过程中制造工艺变量 n 的余量。

高加速极限试验方法是通过促使产品快速失效的方式以识别并减少产品的设计薄弱环节，其目的是提升产品在外场使用过程中的健壮性。该类加速试验不是为了估量产品的可靠性，而是在外场应力（载荷）到产品强度之间余量最小的情况下消除其失效模式来增强产品的可靠性（图 6-16 和图 6-17）。该类加速试验仅仅识别产品潜在的失效模式以指导产品的设计改进过程。从高加速极限试验得到的经验可知，大多数产品在其承受的应力下是非常健壮的，但其内部一些组件或设计细节比其他部分明显要弱，而高加速极限试验的理念就是找出这些组件或设计细节，使其与产品其他部分一样健壮。

图 6-16 说明了产品强度-应力分布的交集，图中的分布是正态分布。产品的强度随着原材料和生产过程的变化而变化，可用强度模型来表示。

应力分布和强度分布的重叠区域表征了产品的失效概率。图 6-16 中的曲线表示了经典的设计余量，即应力-强度准则，但在本章没有说明累计损伤模型，因

此，不适用于测定产品设计最终强度的初期短时试验。同样，如果批量产品的质量控制在能够保持在一个非常窄的强度分布内（这是一种费时费成本的方式），那么这两条分布曲线就不会重叠，这就意味着产品在外场不太可能出现某种特定失效模式的失效。

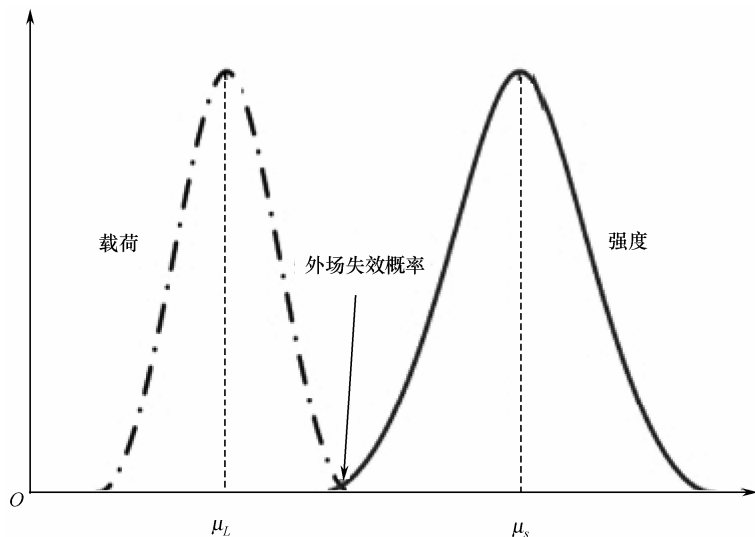


图 6-16 使用载荷和产品强度概率分布密度函数之间的关系

产品的生产过程，特别是在受试组件初样产品的生产过程中，总是保持着严格的生产控制，但在后续产品的生产过程中，可能就不是这样实施的。图 6-17 说明了受试样品通常都可以达到产品的平均强度甚至更高，因为它们通常是在一个投入了最大管理精力的特定原型生产线上所生产。一旦产品进入批生产，常规生产出的产品总是比初样产品的强度较弱，如果精心生产的初样产品的概率分布是应力的函数，那分布曲线的左侧（即 H1 的位置）则成为批生产产品所形成的新分布的均值位置。

初样产品强度分布的分散性较窄，使其远离预期的载荷分布。在这种生产方式下的所有产品均能通过试验而不会发生失效。但在随后的大规模生产阶段，产品的强度均值会显著降低，所以产品强度分布曲线和载荷应力分布曲线的重叠区域就会出现，这将导致生产管理状况较弱的产品在外场载荷的作用下会发生失效，这也意味着该试验不能充分发现批生产产品的潜在薄弱环节。如果试验的应力水平更高（均值接近图 6-17 中 H3 的应力水平），且在产品强度分布中包括常规生产的产品，则该试验可以提供充足的余量以确保产品薄弱单元的潜在失效能够被发现并减少。在没有充足余量的情况下，将会导致随后生产的产品在外场发生失效。

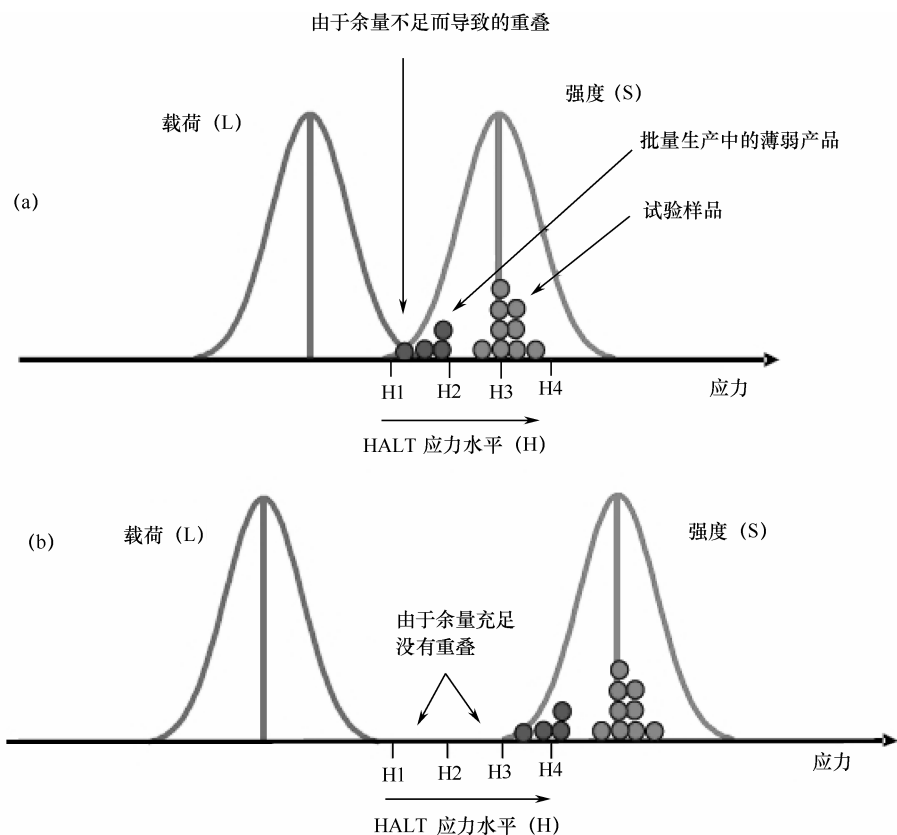


图 6-17 增加应力以检测和缓解薄弱环节，并增加应力和余量

这就是应用步进应力和高加速极限试验的原理，以确保有合适的超过产品寿命期内预期应力的余量。通过这种方式，这些试验所需的试验样品比传统试验所需的试验样品少得多。

高加速极限试验是一种研制性质的、定性的设计改进试验，应该被人们所接受。它可在相关的应力类型下识别产品设计中最薄弱环节的失效模式。如果这种失效模式与产品使用环境中的应力相关，该应力水平仅仅依靠工程经验来判断，则要考虑载荷与产品强度曲线之间的余量，并考虑因生产工艺、预期使用环境的变化而增加的额外余量。

随着高加速极限试验的开展，首先是最薄弱环节失效，接着是第二、第三及其他相对薄弱环节失效，直到不再发生相关的失效模式或达到了受试系统的技术极限为止。

高加速极限试验所施加的应力被设计成远远超出产品的使用环境应力和设计规范规定的应力。这种应力持续时间短，其目的就是促使产品的薄弱环节转化为失

效，并在技术和经济方面都切实可行的情况下健壮产品。高加速极限试验是识别产品的失效模式，而不是确定产品的时间依赖性。

在试验过程中，必须监测受试单元的功能特性以便发现其是否存在功能缺失。如果无法对其进行连续监测，那么应在应力水平保持恒定的时刻对产品功能进行测试。

应力量值并不是高加速极限试验最关心的问题，一个有效的高加速极限试验规划真正关注的焦点在于产品改进工作和对产品失效的组织响应上。对产品持续地改进直至达到费效比平衡点为止，即产品设计的各个部分没有明显比其余部分薄弱，其目标是持续改进产品直至商业角度和费效分析技术所确定的合理水平为止。

产品的工作应力极限和破坏应力极限可在应力轴上绘制成分布曲线，如图 6-18 所示。

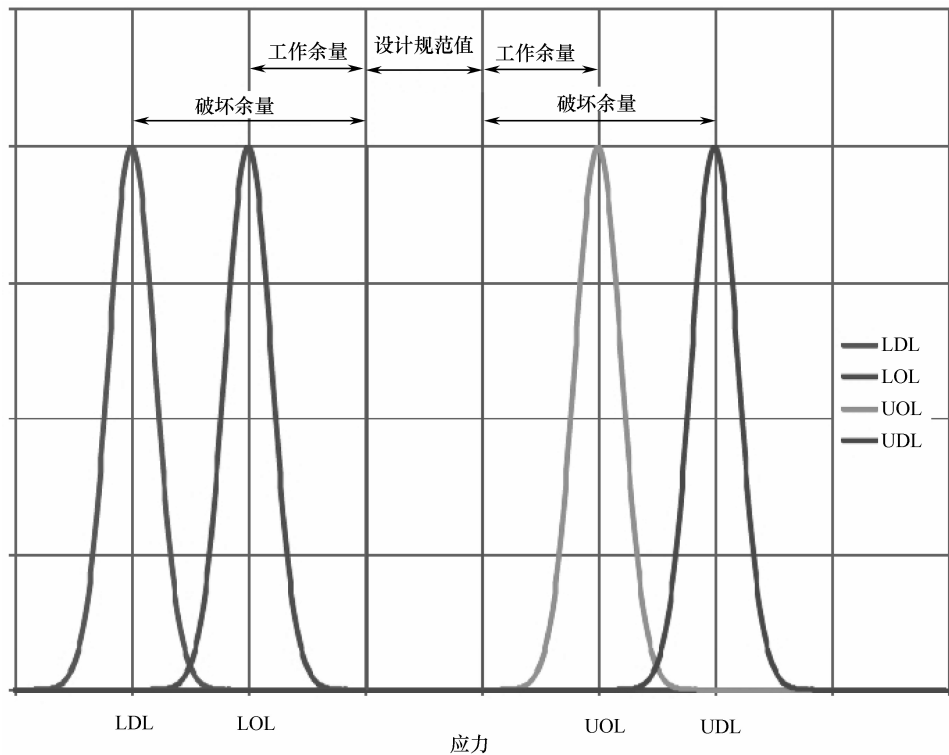


图 6-18 以应力概率密度函数表示的工作应力及破坏应力极限

图 6-18 是一个应力上下限都影响的产品实例，有上限和下限这两种应力极限（工作极限下限 LOL、工作极限上限 UOL、破坏极限下限 LDL 及破坏极限上限 UDL）。例如温度应力，高温和低温都影响产品的性能。由于高温及低温极限与设

计标称温度的距离不同,因此这些影响可能没有对称性。即使在可提供产品设计相关失效模式信息的初样品上进行试验也是如此。所有这些分布可能具有不同的标准偏差,确定开展高加速极限试验也就预示着产品有一定的应力余量,这个余量使最终产品适应外场各种应力的变化而不会发生失效。

对于某一种产品而言,描述产品的各种应力极限如图 6-19 所示。



图 6-19 产品的各种应力极限示意图

工作极限 (Operating Limit) 和损坏极限 (Destruct Limit) 的几个具体定义如下。

- 工作温度下限——温度降低到产品停止工作或不再满足技术条件要求,但温度上升后,产品仍能恢复正常工作的那个温度值。
- 损坏温度下限——温度降低到产品停止工作或不再满足技术条件要求,且温度上升后,产品已不能恢复正常工作的那个温度值。
- 工作温度上限——温度升高到产品停止工作或不再满足技术条件要求,但温度下降后,产品仍能恢复正常工作的那个温度值。
- 损坏温度上限——温度升高到产品停止工作或不再满足技术条件要求,且温度下降后,产品已不能恢复正常工作的那个温度值。
- 工作振动极限——振动强度加大到产品停止工作或不再满足技术条件要求,但振动强度下降后,产品仍能恢复正常工作的那个振动强度值。
- 损坏振动极限——振动强度加大到产品停止工作或不再满足技术条件要求,且振动强度下降后,产品已不能恢复正常工作的那个振动强度值。

即使图 6-18 和图 6-19 描述的是温度应力,其他应力也可成功应用在高加速极限试验中。在其他应力类型的情况下,应力极限的下限可能不存在,如机械应力,但其他应力有可能存在,如电应力和湿度等。

为了保证试验的有效性,HALT 试验必须在能够代表设计、元件、材料和生产所使用的制造工艺都已落实的样件上进行,这样才能充分发现设计的薄弱环节,更准确地分析产生这些缺陷的根本原因。另外,HALT 是采用步进的应力逐步激发试

件的缺陷，从而使试件表现出某种形式的失效。如果以所施加应力为 X 轴，以失效的试件数为 Y 轴，且参加试验的试件足够多，就可以得到如图 6-20 所示的统计曲线。HALT 试验的目的是为了发现产品设计的薄弱环节，从图中可以看出，在 HALT 试验中要发现某种失效形式，推测产品工作和破坏极限，并不需要太大的试验样本，在试验中只要对所选试件不断增大应力，它总会在上述曲线的某一位置出现失效，从而发现这种缺陷类型。为了保证试验中出现的失效形式具有代表性，能验证某失效模式不仅仅是在某一单个样件上出现，又不至于因为 HALT 是一个破坏性试验而造成浪费，所以在 HALT 试验中一般采用小的样本数（典型的是 4~6 个）就够了。

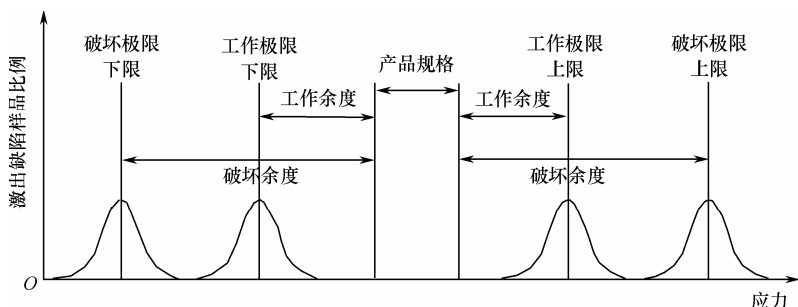


图 6-20 HALT 试验中应力量级与激出缺陷样品对应比例

3. 应力类型及应用

在高加速极限试验中，主要的或典型的应力有：

- 温度。
- 热循环。
- 振动/冲击。
- 电压。
- 振动/冲击及热循环的综合应力。

在高加速极限试验中，也可应用其他特殊应力，如微处理器的时间脉冲频率、电压、电源波动、污染物、溶剂等，或上述这些特殊应力的综合应力。

通过高加速极限试验验证产品的应力余量，以及对产品进行的改进有益于提高产品外场使用时的健壮性和可靠性。

最大应力可按以下几方面进行确定：

- 所用材料、组件的材料极限和技术极限。
- 现有的方法和设备所能达到的最大应力。

需要注意的是，所施加的应力水平不得超过使材料的物理或化学特性可能发生

变化的强度极限。

通常情况下,在受试单元中存在一些较脆弱的元件,而这些元件本身就不是为无法承受高加速极限试验中所施加的应力水平所设计的,因此,在可能的情况下,应在高加速极限试验过程中对这些较脆弱的元件进行保护,或在试验数据评估时将其予以剔除。例如,可对较脆弱的元件施加冷却空气,或与冷空气隔离,或使元件悬浮于受试单元的外部以便使其避免承受振动和冲击,甚至可将元件移到高加速极限试验箱外,并用延长的信号线将其与受试单元的其他部分相连接。

在高加速极限试验中发现的每一个失效应该进行调查并从根源上分析原因。若所发现的失效模式可能会在现场外场(其应力水平低于高加速极限试验的水平)应用时出现,那么应从工程技术及产品管理的角度来决定采取相应的纠正措施。

下面举例说明加速应力的剖面设计。

(1) 温度步进 (Temp Step Stress)

此项试验分为低温及高温两个阶段应力,首先执行低温阶段应力(Low Temp Step Stress)。将待试验样品放于 HALT 试验箱中,将温度感应线接至欲记录的零件上,并调整风管使气流能均匀分布于机台上,根据待试验样品的电气规格加满载,设定起始温度 20°C ,每步段降温 10°C ,每步段温度稳定后维持 10 分钟,在每步段稳定温度时执行至少一次的通断电启动及拉载测试,如一切正常则将温度再降 10°C ,并待温度稳定后维持 10 分钟,再执行上电启动及拉载测试,依次类推直至发生功能故障,将温度恢复至常温并稳定后,再执行上电启动及拉载测试,观察其功能是否恢复,以判断是否达到工作极限或破坏极限,如功能正常恢复,则将故障前的低温值记录为工作极限,同时再将温度逐段下降直至发现当恢复常温仍然无法使功能自动恢复的低温,则此低温即为低温破坏极限。

在完成低温应力试验后,即可依相同程序执行高温应力试验,即将 HALT 试验箱自 20°C 开始,每阶段升温 10°C ,待温度稳定后维持 10 分钟,而后执行通断电启动及拉载测试,直到发现高温工作极限及高温破坏极限为止,如图 6-21 所示。

(2) 快速温度循环 (Rapid Thermal Transitions)

此试验将先前在温度步进所得到的低温及高温工作极限定为此处的高低温度界限,并以每分钟 60°C 的快速温度变化率在此区间内进行 6 个循环高低温变化,在每个循环的最高温度及最低温度都停留 10 分钟,使温度稳定后再执行通断电试验及拉载测试,如发现待测物发生可恢复性故障,则将温度变化率减少 $10^{\circ}\text{C}/\text{min}$ 后再执行温度循环,直到 6 个循环皆无可恢复性故障发生,则此温度变化率即为此试验之工作极限,在此试验中不需要寻找破坏极限,如图 6-22 所示。

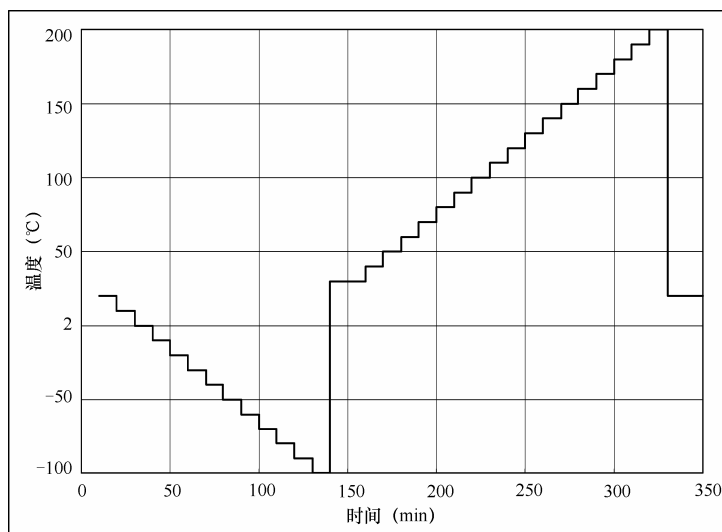


图 6-21 温度步进 (Temp Step Stress) 试验剖面

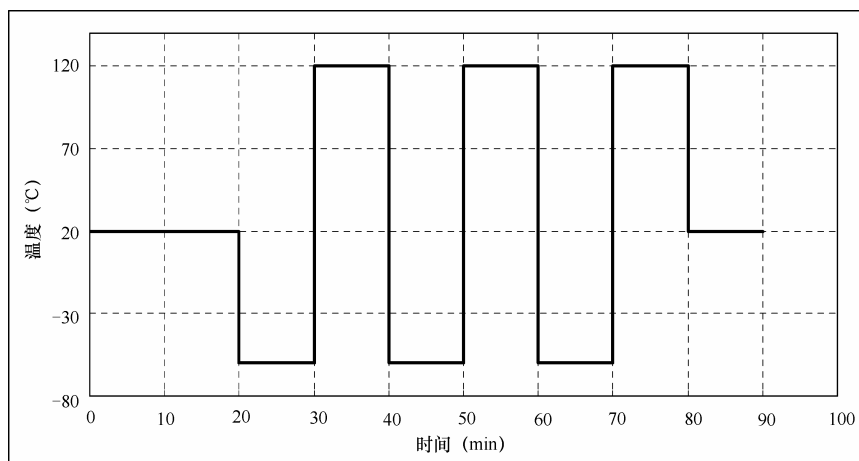


图 6-22 快速温度循环试验剖面 (三个循环)

(3) 随机振动 (Random Libration)

此试验是将振动 G 值自 $5G$ 开始, 且每阶段增加 $5G$, 并在每个阶段维持 10 分钟后, 在振动持续的条件下执行通断电试验及拉载测试, 以判断其是否达到可工作界限或破坏界限。如果正常, 则每次加速度增加 $10G$, 进行指标测试和功能测试, 直到出现异常 (当加到 $40G$ 时, 步长为 $5G$)。当振动加速度超过 $20G$ 时, 每个振点结束, 将振动值降低至 $10G$, 停留 5 分钟, 进行性能测试, 然后进行到下一个振点。出现故障时, 停留 5 分钟, 进行性能测试后, 观察其功能是否恢复, 以判断是否达到操作界限或破坏界限, 如图 6-23 所示。

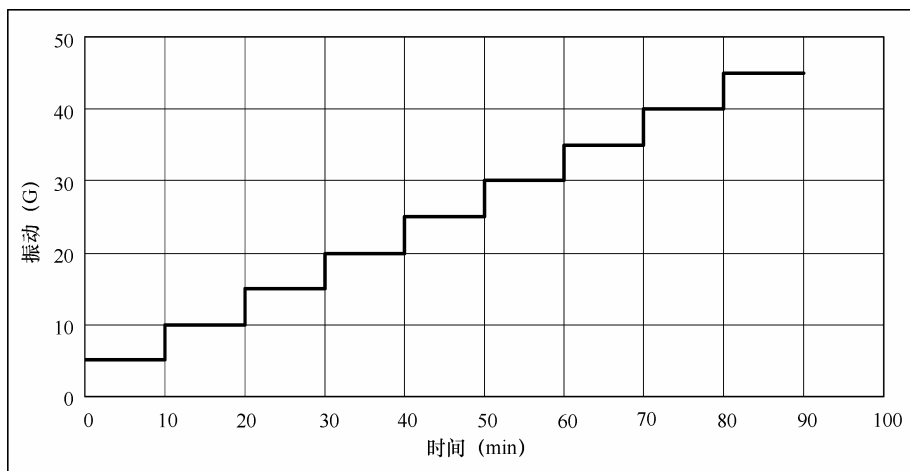


图 6-23 随机振动试验剖面

(4) 综合环境应力 (Combined Environment of Temperature and Vibration)

此试验将使快速温度循环及随机振动同时进行，使加速老化的效果更显著。在 HASS 的实验中需要以综合环境应力的条件执行，方能在短时间内发现制造上的问题。此处使用先前的快速温变循环条件及温变率，并将随机振动自 5G 开始配合每个循环递增 5G，且使每个循环的最高及最低温度持续 10 分钟，待温度稳定后执行通断电及拉载测试，如此重复进行直至达到可工作界限及破坏界限为止，如图 6-24 所示。

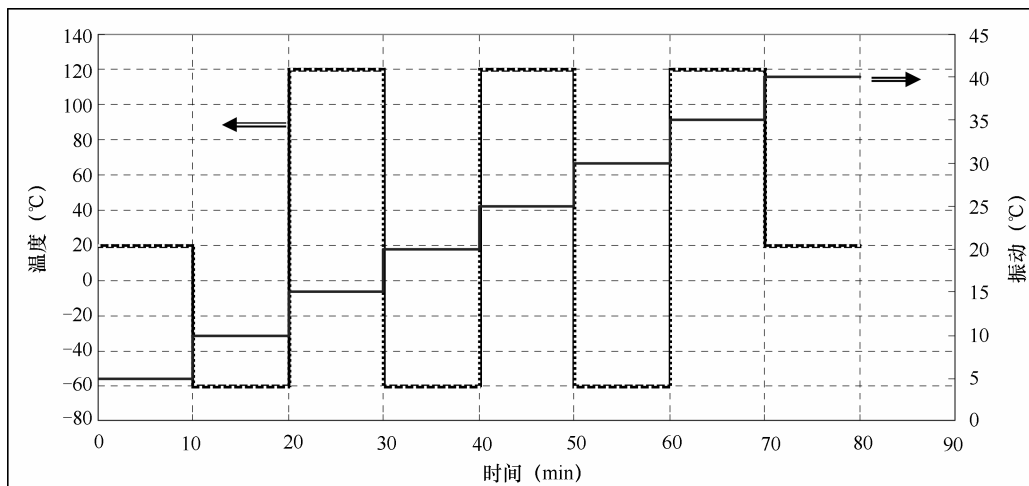


图 6-24 综合环境应力试验剖面

在以上 4 个试验中应对受测物所产生的任何异常状态加以记录，且应分析是否可通过变更设计克服这些弱点，加以修改后再进行下一步骤的测试，提高产品的可

工作界限及破坏界限，从而达到提升可靠性的目的。

4. HALT 的一般程序

HALT 的典型试验步骤如下：

- ① 极限应力水平，如果到达该极限应力试验样件仍没有失效则停止试验。
- ② 安装：将被试设备安装在 HALT 试验箱中，并进行必要的电连接、信号输入/输出连接、监测设备连接等。使用传感器（如温度传感器、加速度传感器等）监测施加在试验件上的应力水平。应该注意的是各种连接应能够承受住试验过程中的应力。在某些试验中，试验件的某一部分不用施加高应力，从而将此部分放在试验箱外，即没有对这一部分进行 HALT 试验；试验件应安装在 HALT 振动夹具上，从而保证振动或冲击剖面能顺利施加到试验件上。紧固夹具不应改变试验箱内空气的快速流动，在某些情况下，可能有必要拆除机箱外壳，从而使箱内气流进入到试验件内部。如果试验件的塑料外壳不能承受高温或高振动加速度，在试验过程中有必要将其拆除。
- ③ 初始化试验：被试设备在 HALT 试验前进行功能测试。监控设备也需要进行测试以确保其功能正常。连接到试验件上的电缆等也需要检查以确保其在高应力（如高的空气流动）下的完整性和正常工作。
- ④ 增加试验应力到规定的应力水平。如果试验件是连续监控的，则应力水平可以持续增加。如果不能连续监控，则应力水平要逐步增加，保证被试设备在每一应力水平下稳定后再进行功能测试，收集可能的失效信息（如果有故障发生）。减小应力，检测试验件的功能是否能够恢复。如果功能可以恢复，则使试验件失效的应力水平就是产品的工作应力极限（OL）。
- ⑤ 继续增加应力水平，直到试验件的功能失效，即使降低应力水平也不能恢复，则该应力水平就是产品的破坏应力极限（DL）。在某些情况下，即使出现了一个永久性损坏（如裂纹），当应力消除时产品的功能仍然可以恢复。此时可以在产品上施加一个小振动量级，运用检测筛选（Detection Screen）对产品进行功能测试来发现或激发间歇故障。找到产品的破坏应力极限后，将其从试验箱中移除，以便能够收集更多的失效信息，确定其失效模式，并找到其失效的根本原因。在某些情况下，进行失效分析的被试设备将不再继续试验。这种情况下，需要用新的被试设备继续进行试验。如果可能的话，出现的故障应该及时修复，并加强产品薄弱部位的设计（如增加支撑或填充材料）或进行保护（如在高温试验中引入冷空气或低温试验中隔绝冷空气等）。在某些情况下，高应力试验中可以对设计的薄弱部分进行保护或将此部分移除试验箱，并保持与试验箱内的其余部分的相关连接。这样可以继续进行试验，以寻找下一个薄弱环节。
- ⑥ 继续进行试验直到找到步骤①中确定的极限应力。

- ⑦ 施加另一类型的应力（如高温），重复步骤②至步骤⑥。
- ⑧ 在工作应力极限范围内重复步骤②至步骤⑥进行循环试验。
- ⑨ 对于传统的 HALT 试验，重复步骤②至步骤⑤进行振动/冲击试验。
- ⑩ 对于传统的 HALT 试验，将步骤⑧中的温度循环与步骤⑨中的振动/冲击试验结合，进行综合应力试验。

⑪ 重复步骤②至步骤⑤进行综合应力试验。

⑫ 进行故障分析，以确定在实际使用中低应力下可能出现哪一种失效模式，评估设计余量时要考虑最严酷的现场条件和制造过程的变更。

⑬ 完成试验报告。当实施了设计改进措施后试验件应重新进行试验，从而证明改进措施的有效性。

⑭ 根据产品的类型及其对应力的敏感性，试验应力的施加顺序可以适当变化。

HALT 施加的应力及顺序是：

- 温度步进，包括低温步进；高温步进。
- 快速温度循环。
- 振动步进应力。
- 综合环境应力。

当失效发生时，应当：

- 暂停试验，记录失效模式和应力水平。
- 定位失效部位。
- 记录失效部位。
- 分析根本失效原因。
- 进行暂时性修复。
- 继续进行试验。

HALT 后的工作，应当：

- 记录所有未定位的问题。
- 与开发者一同讨论试验中的问题，确定纠正责任人。
- 问题修正后，再次验证纠正措施的有效性并没有引入新的失效。
- 周期性评估产品。

【例 6-9】DC/DC 转换器的 HALT 试验及结果分析

表 6-10 列出了某型航空机载 DC/DC 转换器的 HALT 试验条件、结果、故障记录、原因分析和纠正措施等实施情况。

表 6-10 DC/DC 转换器的 HALT 试验结果

试验条件	试验结果	故障现象	可能的故障原因	采取的改进措施
低温	LOT: -70℃（启动） LOT: -76℃（工作） 没有找到其 LDT	启动不稳定	5V 和 3.3V 电源不能在低温条件下正常启动	无；受技术条件的限制
高温	UOT: 125℃ 没有找到其 UDT	12V 电源无输出	产品内部的极限温度使其突然关闭	在软件中设置阈值
振动	OVL: 29.43g RMS 588.6m/s ² RMS VDL: 588.6m/s ² RMS	螺钉松动；电压不稳定	螺钉太松了；手工焊接失效	运用 Loctite 理论改进焊接工艺
-70~125℃之间的温度循环： 4~10min 停留时间	20 个循环后没有发现故障	—	—	—
振动和温度的组合试验：40， 50，60 g RMS -70℃~-125℃	—	印制电路板上掉了三个组件；5V 直流电源故障	—	重新查看生产过程；需要进一步查找故障原因，研究改进措施

5. 高加速应力筛选（HASS）的原理及范围

HASS 并没有被分类为试验，因为它是使用加速应力来筛选出产品的缺陷，而非通过试验对产品进行评价。高加速应力筛选是用显著高于预期使用或运输时的应力来对生产单元进行筛选，但应力水平比能显著降低产品外场寿命的应力水平要低，可基于高加速极限试验的结果确定。筛选试验可在所有的生产单元（100%）上或一个样品上进行。筛选的目的是为了发现产品在正常使用过程中可能出现的潜在缺陷。发现潜在缺陷后，应进行失效分析，并采取必要的纠正措施（通过专门设计的检测特定失效模式的试验进行验证），以降低故障的数量。这样，外场可靠性的提高是由于减少了外场组件制造工艺上的缺陷数量，而非产品固有设计可靠性的改变。

HASS 中的应力水平用于缺陷析出筛选，该缺陷析出所采用的组合应力水平不应超过产品工作应力极限。该类筛选的目的，是为了激发可能导致间歇性或永久性失效的制造缺陷。为发现失效情况，建议在筛选期间监控受试单元的功能，因为受试单元的某些工作异常情况可能在后期的试验检测中无法发现，而且事先也不能确定在筛选期间间歇性功能失效何时发生。析出筛选可能结合了几种应力类型和应力水平。而在高加速极限试验中，间歇性失效可通过探测筛选法进行验证。持续监测应尽可能覆盖产品的所有功能，监测的覆盖率及有效性应在筛选开始前进行优化。监测过程有助于产品失效的根本原因分析。

典型的析出筛选本身所要求的应力施加时间相对较短，约 3 分钟至 1 小时，不

包含试验设备和监测设备的设置时间。

HASS 适用于试生产或扩大生产阶段,即适用于生产速率较低可顺利完成 100% 筛选的阶段。在正常的生产期间,对小批量生产的关键产品,仍可采用高加速应力筛选试验。

在开展试验前,应对试验应力进行选择,以保证产品的功能、材料特性、无缺陷的硬件的寿命不会受损,初始应力水平由高加速极限试验中获取的信息来确定。

因为需要在析出筛选过程中监测受试单元的功能,所以析出筛选的应力水平应略低于工作极限。典型的应力量值为工作应力极限减 5°C ,振动工作极限应力减 $2g_{\text{RMS}}$ 。在 HASS 中采取析出筛选之前,应验证析出筛选不会明显地降低产品的外场寿命,这个可以通过试验验证,比如将一个样品暴露在析出筛选应力中 10 次。

HASS 虽然能够将有缺陷和无缺陷的产品区分开来,以保证不让有制造缺陷的产品流入市场或投入使用,但不是所有的产品都能通过 HASS 过程受益。毕竟 HASS 过程的实现和完成是非常昂贵的,并且经过严格设计、制造和 HALT 试验的产品,其可靠性可能已经满足或超出其最终用户的要求,所以在实际生产过程中,应该通过正确的设计和生产尽量减少 HASS。一般在下列情况下可以考虑利用 HASS 对产品进行筛选:

① 通过 HALT 发现产品的实际裕度比要求的要低,但在产品出厂前又不能解决这个问题。

② 在 HALT 试验中发现产品存在制造缺陷,并且很显然通过环境应力筛选能够提高产品外场可靠性。

③ 复杂程度比较高的产品要求进行环境应力筛选,以满足可靠性的要求。

④ 如果要求通过筛选获得有关产品余度的统计信息,就需要大量的产品进行试验才能得到有意义的统计结果。

⑤ 产品可能有许多不同的组件或部件供应商,当供应商变化时需要通过筛选来衡量所提供的元器件或组件的性能。

⑥ 产品本身就是一个低可靠性的产品。

6. HASS 剖面

HASS 的基本依据是故障物理学,在 HASS 中所施加的应力类型不一定是产品使用时受到的应力,以能激发出制造缺陷为目的,一般选用的应力有振动应力、热应力和电应力等。试验剖面图的建立就是要选择合适的应力类型、应力量级和综合方式,以得到最佳的筛选效果。

(1) 在 HASS 剖面图中选择有关参数的一般方法

HASS 剖面的选择主要依据 HALT 的试验结果,以及产品性能测试所需要的时间、产品试验过程中所施加的特殊应力和产品产量等等。一般的 HASS 剖面图是由

数个在两个极限温度之间的振动和温度等环境应力综合作用的循环周期构成。剖面参数包括：上下极限温度、端点温度滞留时间、温变率、振动量级、振动应力施加时刻、振动时间长短等。这些参数值的选择一般参照下面的方法：

- 温度循环：循环时的高、低温度一般取极限工作温度的 80%，高、低温度点的滞留时间一般取决于试件温度达到平衡所需要的时间和测试试件工作状态所需要的时间。
- 随机振动：振动量级一般是破坏极限的 50%，如果超过了工作极限，则取工作极限的 80%。

在许多情况下，试验剖面图由缺陷激发周期和缺陷检测周期共同构成，激发周期的上下极限值一般在产品的工作极限和破坏极限之间，一般推荐取破坏极限和工作极限的平均值，缺陷检测周期的上下极限值取在产品的工作极限范围之内。

图 6-25 是某通信单元的 HASS 剖面图，它由两个周期构成：第一个周期用来激发产品的各种薄弱环节，应力量级选在产品的工作极限和破坏极限之间；第二个周期紧跟于第一个周期之后，它的应力量级仅低于 HALT 试验过程中所测得的工作极限，在这个过程中可暴露产品的薄弱环节。

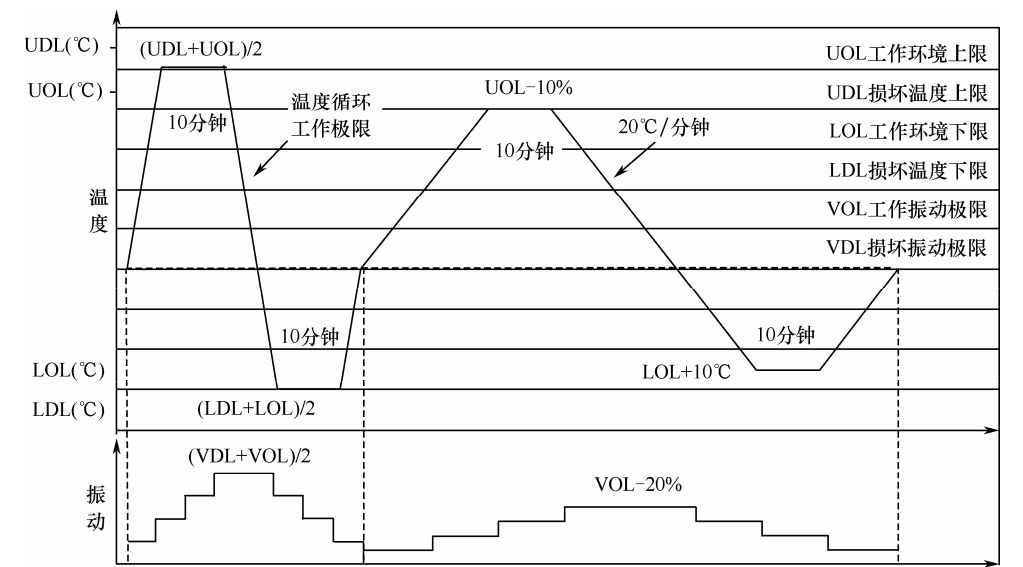


图 6-25 某通信单元的 HASS 剖面图

(2) HASS 剖面图的判定标准和筛选效果的验证

HASS 过程的有效性和经济性是 HASS 剖面图的判定标准，因此 HASS 的筛选过程要保证满足以下两个条件：

- 在 HASS 过程中,所使用的各种应力、应力量级和作用时间能够快速、经济、有效地激发出在正常使用环境下可能导致产品失效的各类缺陷。
- 在 HASS 过程不产生下列副作用:损坏好的产品或产生新的缺陷;过量消耗产品的有效寿命。

筛选效果验证主要是用来证明 HASS 剖面图是否能够满足其筛选判定标准的要求,它包括筛选过程有效性的验证和产品剩余有效寿命的评估两方面的内容。

① 筛选过程有效性的验证。

筛选的有效性是指 HASS 剖面激发潜在缺陷的能力。一般的做法是把有制造缺陷(这些缺陷必须具有代表性,可以人为植入)的试件和好的试件放入试验设备,按照所选择的 HASS 剖面进行试验,对筛选过程中出现的失效形式进行分析,并确定产生这些失效形式的根本原因,以判别这些失效形式是由于在筛选过程中遭受了过大的应力诱发的,还是由于疲劳或制造缺陷造成的,从而决定 HASS 剖面所选择的应力量级是否正确和是否需要修正。如果失效是由于筛选过程中遭受过大的应力造成,则应减小试验剖面中的应力量级,再选用新的试件重新验证筛选过程的有效性;如果预先植入试件的缺陷没有被激发,则可以通过增加试验剖面的应力量级或循环周期来增强筛选强度。

② 产品剩余有效寿命的评估。

这个过程用来评估产品经 HASS 后产品的剩余寿命,或者说用来评价 HASS 是否过多地损伤了产品的有效寿命。评估的一般方法是按照试验剖面的要求将产品重复试验多次,查看是否有失效现象发生,然后从导致失效发生的试验剖面重复周期数可以推断出所选 HASS 剖面对被试产品有效寿命的损伤程度。例如,如果产品通过 10 个 HASS 剖面的循环而失效,那么可以断定该产品经过一个试验剖面的筛选后,产品至少还剩余 90% 的有效寿命,也就是说,通过一个试验剖面的筛选,最多损伤了产品 10% 的有效寿命。在实际应用中一般选取至少 3 个样件,每个样件反复 10~20 次,直至不再出现故障为止。如果要求产品的有效寿命损伤更小,那么重复的次数可以进一步增加。

(3) 建立 HASS 剖面图的一般方法

根据 HASS 剖面有关参数的选择方法和筛选效果的验证方式,在实际中用来开发 HASS 剖面的优化筛选过程常用的方法有以下 4 种。

① 方法 1: 采用预先植入缺陷的样本制订和优化 HASS 方案。

这种方法是将 HALT 试验所测得的应力极限值降低作为初始 HASS 剖面图的应力极限,然后选取好的样件,要求按照该剖面图反复试验 50 次而产品不出现失效。当在试验过程中有失效情况发生时,可降低筛选应力量级,再重新选择好的样件反复试验 50 次,直到没有失效发生为止。要求重复 50 次而不出现失效是为了保

证最后的 HASS 剖面图所采用的应力量级不是太大，以便保证在筛选过程中不损伤好的产品。这个过程完成以后，再按照 HASS 剖面图对有植入缺陷的样本进行筛选试验，看在筛选过程中能否充分暴露这些人为植入的缺陷，以保证最后所确定的筛选应力量级足够大。这种方法的好处是它往往只需要一套试件就能够完成整个 HASS 剖面的开发和优化过程。但这种方法的不足之处是需要几个具有植入缺陷的样本（这些样本植入的缺陷是制造缺陷，包括冷焊和有刻痕的管脚等），并且完成整个开发过程大概需要 4 天的时间。在实际应用过程中，对样本植入各种缺陷或在外场、生产线发现能代表该产品所有制造缺陷的样本很难，植入的缺陷往往只能代表制造缺陷类型的一部分，对那些在筛选过程中极难发现的缺陷难以植入，因此按照这种方法制订的 HASS 方案难以保证将工艺过程中的所有缺陷激发和暴露。当试件能够成功植入各种制造缺陷，或能够从外场、生产线上发现这样的典型样本时，这种方法是非常理想的。

② 方法 2：采用小样本数制订和优化 HASS 方案。

同方法 1 一样，这种方法也是将 HALT 试验所测得的应力极限值降低作为初始 HASS 剖面图的应力极限，然后选取好的样件，再按照该剖面图反复试验 50 次而不出现失效。当有失效情况发生时，可将筛选应力量级降低，再重新选择好的样件反复试验 50 次，直到在这种情况下没有失效发生为止。如果采用初始 HASS 剖面图反复试验 50 次没有出现失效，则将 HASS 所确定的应力极限值增大，直到有失效情况发生，这是为了保证筛选过程中所采用的应力量级足够大。这种方法的优点是：在开发和优化 HASS 过程中只需要一套试件；缺点是这个过程比方法 1 需要更多的时间。如果被筛选产品很昂贵，可获得用来进行 HASS 过程开发的试件数很少，并且在外场使用中产品的可靠性又很关键，采用这种方法优化 HASS 剖面图是非常理想的。

③ 方法 3：采用大样本数制订和优化 HASS 方案。

在这种方法中，HASS 过程所采用的初始应力值略低于 HALT 试验中所得到的破坏极限，然后选取好的样件、按照试验剖面图反复试验 50 次而不出现失效。如果有失效情况发生，可将 HASS 应力值不断调低，直到筛选过程按照试验剖面图重复 50 次而被试产品不出现失效为止。因为在这种方法中所采用的筛选初始应力值接近产品的破坏极限，所以很容易发生失效。这种方法的优点是：可以确信用该方法确定的 HASS 过程足够强壮，能暴露更多的产品缺陷。缺点是：它需要 3~4 套产品，并且完成确认 HASS 剖面图的开发比方法 1 和方法 2 需要花费更多的时间。如果产品造价很低，可提供很多的试件供开发 HASS 的筛选方案使用，且在外场使用过程中产品的可靠性非常关键，采用这种方法开发和优化 HASS 剖面图是非常理想的。

④ 方法 4: 只对产品有限样本进行筛选的 HASS 方案。

方案的制订和优化的方法与方法 1 及方法 2 一样,这种方法也是将 HALT 试验所测得的应力极限值降低作为初始 HASS 剖面图的应力极限值,然后选取好的样件,按照该剖面图反复试验 50 次而不出现失效。当有失效情况发生时,可将筛选应力量级降低,再重新选择好的样件反复试验 50 次,直到在这种情况下不出现失效现象为止。如果采用初始 HASS 剖面图反复试验 50 次没有出现失效,初始试验剖面图就直接被采用,而不需要再进一步的改进。

这种方法的优点是:采用这种方法开发 HASS 剖面往往只需要一套试件就够了,并且整个过程只需要花费大概 2 天的时间。缺点是:不能证明它足够强壮,即这种试验剖面图能否检测到微小的工艺或加工过程的变动,不得而知。当采用 HASA(高加速应力鉴定)方法对产品进行筛选时,用这种方法来制订筛选方案是非常有效的,因为 HASA 的目的是为了对产品的制造缺陷进行粗略筛选,所以即使筛选应力量级低一点,也还是能检测出这些缺陷的。

7. 产品 HASS 的实施过程

和 HALT 试验层次性要求一样,要有效实施 HASS,彻底清除产品的早期故障,应该在能够产生加工缺陷的元器件级、模块级、单元级和系统级按照从低到高的层次进行 HASS,才能保证整个产品的可靠性。

当产品某层次的 HASS 剖面图被建立和验证后,就可以按照它对产品施加应力并开始筛选,以区分出有缺陷和无缺陷产品,分析失效机理,为改进产品提供有用信息。在筛选实施阶段要注意以下几点。

① 进一步对 HASS 方案的优劣进行考证。

在整个 HASS 过程中不仅仅要求在开始或结束时收集失效率数据,还有记录失效出现的时间,绘制出 λ -t 图,来考究产品的 HASS 方案。如果曲线不变或随时间上升,那么 HASS 程序无效,这可能是因为没有早期失效缺陷或筛选应力/应力量级不当造成的,然后分析原因,对 HASS 方法进行改进。

② 改进产品,减少或消除筛选过程。

因为环境应力筛选是一个鉴定的过程,它不会使产品增值,所以应尽快减少或消除。如果 HASS 程序制订得当,在筛选过程能深入分析失效机理,及时采取修正措施,就会使产品不断得到改进,最后使早期失效大大减少或消除。

③ 利用筛选过程,检验产品改进措施。对于改进后的产品,在筛选过程中也要进一步收集和分析 HASS 数据,如果改进措施得当, λ -t 曲线中早期失效区应当变小,这是由于在较短的时间内达到失效率不变的稳定期。如果产品改进后曲线不是这样,则说明改进措施不得当,应立即反馈给有关技术人员。



④ 在 HASS 过程中,为满足产品批量生产的要求,必须认真设计测试系统的软、硬件,在满足多通道数据采集的同时,尽量不过多衰减反映产品工作状态的信号,满足试件数量多和测试数据准确性高的要求。

⑤ 在进行温度循环时,要保证试验中所使用的电缆能经受住试验中所施加的热应力。许多商业电缆能承受的温度一般是 105°C ,长时间的高温冲击 ($>110^{\circ}\text{C}$) 可能熔化或软化电缆表皮。高温有可能使电缆承载电流的能力降低,低温会使电缆变脆,使其不能够经受其试验过程中的振动。还有在试验中的连接器要保证在温度循环和振动应力作用下不产生断断续续的导通现象。

6.6.4 加速试验的局限性

可靠性加速试验方法的局限性主要如下:

① 加速因子的确定非常复杂,需要耗费很大的时间和成本,因此,获得的加速试验时间和可靠性指标(主要依赖于加速因子)的精度有限。

② 有时很难推断出综合应力中哪一个应力导致了某一特定的失效模式发生,以及对该失效模式的影响程度,因此试验过程中可能高估或低估加速因子的综合影响。

③ 试验样本有可能过大或者太昂贵。在这种情况下,样本量不能满足试验要求,使得试验的置信水平不高。

④ 试验设备特别是那些自动测试、监控设备,由于太复杂以至非常昂贵或不易管理。

⑤ 由于样本中大的热量块或者应力比的局限性,一些加速试验手段可能无法实现,因此,由于缺乏有效的加速,试验可能要耗费巨大的时间和成本。

⑥ 在高加速极限试验 (HALT) 中,试验样本量一般只有 1~6 个,不能代表所有产品的平均强度水平。而且个体的破坏性极限也不相同,小样本量试验有可能得出错误的结论,也有可能试验样本的强度要高于产品的平均水平。

⑦ 在元件的试验中,一般是基于失效时间确定其失效曲线,而这些曲线又用于确定加速试验条件以及为元件的可靠性评估提供信息。当元件很小且在试验中完全被破坏时(烧毁或其物理性能遭到了极大改变),通常无法确定是哪一种失效模式导致其失效,因此试验结果拟合得到的分布可能是错误的,从而提供了错误的可靠性信息。

⑧ 加速试验得到的信息与试验中的应力及各应力组合有关,因此,如果该产品以不同的方式或在不同的环境中使用时,试验结果不能用于评估其可靠性,必须重新进行试验。

⑨ 由于产品可能在与试验应力不同的应力水平下使用,通过加速试验得到的量化评估结果有可能不能用于预计单个产品的可靠性。

参 考 文 献

- [1] 张增照. 以可靠性为中心的质量设计、分析和控制. 北京: 电子工业出版社, 2010.
- [2] 祝耀昌. 可靠性试验及其发展综述. 航天器环境工程, 2007, 24(5): 261~269.
- [3] 任占勇, 祝耀昌. 可靠性加速试验技术与传统可靠性试验技术的对比分析. 航空标准化与质量, 2001, 6: 35~39.
- [4] 蒋成彬. 可靠性增长测定试验探讨. 雷达与对抗, 1999, 3: 67~72.
- [5] 王欣, 任占勇. 电子产品可靠性增长摸底试验——方案的确定方法及实施要求. 航空标准化与质量, 2001, 2: 27~31.
- [6] 张志华. 加速寿命试验及其统计分析. 北京: 北京工业大学出版社, 2002.
- [7] 金星, 等. 可靠性数据计算及应用. 北京: 国防工业出版社, 2003.
- [8] GB 5080.5-85. 设备可靠性试验: 成功率的验证试验方案.
- [9] GB 5080.6-89. 设备可靠性试验: 恒定失效率假设的有效性检验.
- [10] GB 5080.7-87. 设备可靠性试验: 恒定失效率假设的 MTBF 验证试验方案.
- [11] GB/T 15174-1994. 可靠性增长大纲.
- [12] GB/T 1772-79. 电子元器件失效率试验方法.
- [13] GB/T 2689.1-1981. 恒定应力寿命试验和加速寿命试验方法总则.
- [14] GB/T 5329-1985. 试验筛与筛分试验术语.
- [15] GJB 1407-1992. 可靠性增长试验.
- [16] GJB 899A-2009. 可靠性鉴定和验收试验.
- [17] GJB 1032. 电子产品环境应力筛选方法.
- [18] IEC 62506: 2013 Methods for product accelerated testing.
- [19] 褚卫华, 陈循, 陶俊勇, 等. 高加速寿命试验 (HALT) 与高加速应力筛选 (HASS). 强度与环境, 2002, 29 (4) .
- [20] 蒋瑜, 陈循, 陶俊勇. HALT 试验高效率振动剖面的建立. 宇航学报, 2006, 27 (3) .
- [21] 林震, 张爱民, 沈朝晖, 等. 谈谈高加速寿命试验. 环境技术, 2002 (4): 5~9.
- [22] 林洁. 现役设备可靠性增长的办法. 第三届电子产品可靠性与环境实验技术经验交流会论文集, 2001.

第7章

可靠性数据收集与分析

7.1 概述

7.1.1 数据、信息的概念及特征

1. 数据、信息的概念

“数据”和“信息”在日常表达中通常作为意思相同的术语而相互换用，但实际上，这两个术语有着明显不同的含义：

- 数据是指记录的事实、事件及事务等，是获得信息的原始材料。它们可以以数字、图表、符号、文字、曲线、电子文档等形式存在。
- 信息是经过某种方式加工得到的、对接受者有用的数据。

总而言之，基本的数据经过某种方式处理而形成信息，但没有特定目的、纯粹的数据处理活动本身并不产生信息。

2. 数据的特征

数据是指通过读取、观察、计算、测量、称重，以及自动采集等方式获得、随后被记录的事实。这些数据通常被称为原始或基本的数据，经常是一个组织（机构）日复一日的事务记录。

数据来源有内部的和外部的。大多数的外部数据具有易用、具体的形式。而组织内部活动事实往往需要适当的测量和记录系统才能获得。数据可能是一些日常事务自动产生的副产品，但必须纳入如入库登记、特定的计数或测量程序这样一些基本事务，并记录结果。大多数成本核算、库存控制、产品控制及类似系统都属于后一种情况。

通常，人们对数据处理过程会给予相当多的关注，而对原始数据的质量却错误地认为是理所当然的。如果原始数据本身是有缺陷的，由此得到的任何结果信息都是毫无价值的。

一个组织来自其内部和外部数据源的可用数据集是无限的。如此丰富的数据资源带来了问题，这就要求必须从收集的数据中加以挑选。此外，数据收集机构还必须监控其数据收集流程，以确保其能持续满足特定需求。

3. 信息的特征

就其精确定义而言，信息的概念比日常使用的这个通俗词语的意思要复杂和难以理解。信息是被其接受者所充分诠释和理解的数据。值得注意的是，不只是信息的发送者，还有其使用者也会介入数据转换为信息的过程。在转换的过程中涉及思考和理解的过程，其结果是一个给定的消息对不同的人有不同的意思。还有对数据进行分析、总结或者用其他方式处理而得到的消息或报告，通常被认为是“管理信息”的数据，这些数据只有被其接受者所理解才称之为信息。只有使用者才能确定一份报告是否包含信息或者只是处理过的数据而已。

信息除了具有提升知识的一般作用外，在工程应用中还有以下几方面的作用：

- 减少不确定性：不确定性的存在是因为根本不存在完备的认识，但相关信息有助于减少未知因素，这在很大程度上与制订计划和决策有关。
- 作为一种监视和控制辅助工具：通过提供执行情况及其与计划的偏差程度信息，管理部门可以更好地控制业务运作。
- 作为一种交流方式：管理者需要知道的工作计划、发展状况以及即将发生的变化等信息。
- 作为记忆的一种补充：通过拥有以往相关活动的执行、处理、结果和可参考决策的历史信息，人的记忆得到了补充。
- 通过减少不确定性和加强理解，可作为一种简化的辅助手段，使问题及态势得到简化而变得更易管理。

信息本身没有价值，其价值来源于根据有效信息作出决策行为引起改变的价值与产生信息的成本之差。一般而言，信息越多、越早、越新或者越准确越好。信息只有当其改进了结果决策时才是好信息，否则，信息就没有价值。

无论如何，数据的获取、处理、记录、加工等过程都需要成本但不会产生价值。只有当数据传达至其接受者，并被其理解而转化为信息，信息被用来改进决策的制订时，其价值才会产生。

好的信息是指被使用并能产生价值的信息。衡量好信息主要有以下标准。

(1) 相关性

实质上，这是顶层性质。信息必须与所考虑的问题相关，但很多时候是报告、消息、表格等，往往包含了不相关的内容，这使得用户对问题的理解更加困难。相关性在很大程度上受到下列许多性质的影响。

(2) 准确性

考虑到管理者对信息的依赖和信息的利用目标，信息必须足够的准确，不存在绝对准确这种情况，而且，提高准确程度会增加成本，但并非一定会增加信息的价值。信息准确程度必须与其涉及的决策的层次相关联。在操作层次上，有关失效时间的信息需要准确至最接近的分钟；在战术层次上，此信息可能最恰当的是准确到与之最接近的天数；而在战略层次上，则通常只需准确到最接近的三个月即可。不能将准确与精确混淆了。信息有可能是不准确但精确的，反之亦然，如图 7-1 所示。

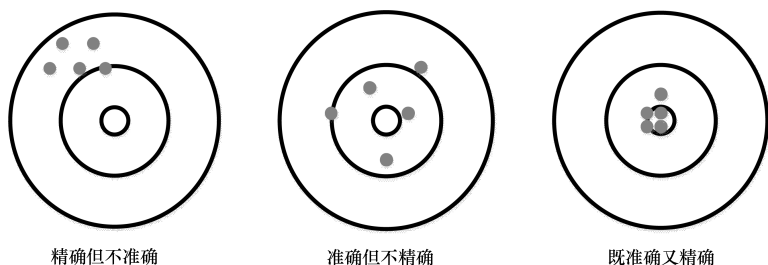


图 7-1 准确与精确之间的区别

(3) 完整性

理想的情况是，决策所需的所有信息都能得到，但事实上这永远是不可能的。实际上，需要的只是对于问题关键因素方面的信息完整。这就意味着信息的提供者 and 使用者应有紧密的联系，以确保信息的关键因素得到确认。

(4) 来源的可信任性

信息必须被利用才有价值。信息的使用者必须对其所使用的信息来源有信心。当以往的使用证明其来源可靠时，或者当信息的提供者与使用该信息的工程师有较好交流时，这种信心会随之增加。通常理论上（想定的）的一个确定值，可作为提供者和使用者对数据项信心的一个随意但相关的尺度，用以评价每个数据项。在数据处理的时候，把这个确定值加以考虑（确定值低的数据可能被忽略），可得到经处理信息的好坏程度的尺度。

(5) 传递到合适的人

每个人经常都有特定的活动领域和责任，并接收信息以帮助其完成所指派的任务。实践中这并不像听起来那么容易。信息总是提供给了组织中错误的层次，这

种情况太常见了。一个较高职位的人可能不会将信息传递给真正需要的人，而一个较低职位的人也有可能会握住信息不放来试图证明自己是不可缺少的，因此，信息的提供者需要分析组织中的关键决策点，以确切指明究竟是哪里需要信息。

(6) 适时性

好的信息在被利用时得到传递。虽然在一定程度上，现代化的数据处理方法能够快速产生准确的信息，但对传递速度的要求可能会与对信息准确性的要求相冲突。数据在收集、处理或传递方面的延迟可能会将潜在的重要信息变为毫无价值的废纸。定期产生数据的时间选择也很重要。信息需要以一定的频率产生，这个频率与其涉及的决策类型或活动有关。通常，在没有考虑所涉及活动的时间周期时，报告是例行地以非常任意的间隔（如每天，每周，每月等等）产生的。在操作层次，这可能是指信息可持续获得的需求，但在其他层次上，更长的间隔可能会更合适一些，这种间隔不能仅仅由日历上的习惯来决定。

(7) 详细性

为做出相应的有效决策，信息必需包含所需的最少数量的细节。而每个多余的特性则意味着要进行额外的存储，更多的处理，额外的消化，也许还有乏味的决断。信息的详细程度应随其在组织中的层次而变化：在组织中的层次越高，其摘要和概述的程度就越高。有时，尤其在较低层次，信息需要非常详细才会有用。但总的原则是，在满足其应用有效的情况下，信息越精炼越好。

7.1.2 数据的收集与分析

可靠性数据的收集和分析处理在可靠性工程中具有重要的价值和作用，也是可靠性工程最为基础的重要工作。可靠性在很大程度上发源于统计科学，与数据存在着不解之缘。我们平时说的“让数据说话”，就是强调数据的重要性。

可靠性数据是指在各项可靠性工作及活动中所产生的描述产品可靠性水平及状况的各种数据。可靠性数据通过某些方法处理和分析，可产生有用的可靠性信息。定量评估产品的可靠性是可靠性数据分析的重要工作之一。由此提供的信息，将作为预防、发现和纠正可靠性设计以及元器件、材料和工艺等方面缺陷的参考，在可靠性工程中发挥着重要的作用。随着可靠性工程的深入发展，可靠性数据及其分析工作的价值/作用显得越来越重要。人们深刻地认识到：有效的数据和信息是开展可靠性、维修性、保障性分析的基础，没有数据和信息，可靠性工程将无法进行。

可靠性数据及其分析伴随着产品寿命周期的各个阶段可靠性工作进行。为了进行方案的对比和选择，在工程研制阶段需要分析同类产品的可靠性数据，该阶段研究和试验



产生的可靠性数据分析结果，可为产品的改进和定型提供科学的依据；为了分析产品的设计和制造水平，在生产阶段需要进行可靠性数据的分析和评估；为给产品的设计和制造提供较权威的评价，需在使用阶段进行可靠性数据的分析，由于其反映的使用及环境条件最真实，参与评估的产品数量较多，所以其评估结果可以反映出产品趋向成熟期或到达成熟期的可靠性水平，是该产品可靠性工作的最终检验，也为今后新产品的可靠性设计和改进原产品设计提供了最有益的参考。由此看来，可靠性数据的分析在可靠性工作中是一项基础性工作，在产品寿命周期的各阶段都发挥着重要作用。

7.2 可靠性数据的重要性

可靠性数据是指在各项可靠性工作及活动中所产生的与产品可靠性水平及状况相关的各种数据，它们可以是数字、图表、符号、文字、曲线和电子文档等形式。广义的可靠性数据包含可靠性、维修性、保障性、测试性、安全性和环境适应性方面的数据。产品的可靠性数据是进一步开展产品可靠性工作的基础，是提高产品质量、进行产品可靠性设计和分析，以及开展产品可靠性试验研究的必要基础。有效地分析和利用可靠性数据、信息，有助于元器件本身的可靠性提高和其评价的准确度，尤其有利于整机及系统的可靠性设计、可靠性预计和可靠性评估。例如：整机产品的可靠性可以反映产品在不同寿命阶段的可靠性状况，以及各种有关因素对产品可靠性的影响和其变化规律，它是进行可靠性设计、试验管理，以及提高和保障产品可靠性的重要依据，它还是开展新品可靠性设计、试验、评审，实现可靠性增长必不可少的支撑。

数据是衡量产品特性的量值，在产品寿命周期的各个阶段都会产生大量的可靠性数据。产品是否可靠，现场使用及试验数据最有说服力，充分翔实的数据更能对产品的可靠性做出客观评价。通常用平均故障间隔时间（MTBF）来说明电子设备的可靠性水平；用失效率来说明元器件的可靠性水平；产品的失效信息暴露了产品本身的缺陷，那么分析产品的可靠性问题必须以产品的失效信息和数据为依据，找到影响可靠性的关键因素，才能采取针对性的纠正措施。随着可靠性工作的深入发展，可靠性数据的收集与分析工作越来越显示出其重要的价值和作用。有效的数据和信息是开展可靠性分析的基础，是决策的依据，没有数据和信息，可靠性工程乃至整个型号的研制工作就好像是无本之木、无源之水。因此，可靠性数据的收集与分析在可靠性工程中有着重要的地位和作用。在可靠性数据收集与分析方面，国外制订了一系列的技术标准，如国际电工可信性委员会（IEC TC 56）专门制订了现场可信性数据收集方面的应用指南（IEC 60300-3-2:2004 Dependability management-Part3-2: Application guide—Collection of dependability data from the field）；我国对可

可靠性的数据收集、管理和分析工作十分重视,在 GJB 1686-1993《武器装备质量与可靠性信息管理要求》中对信息的收集与管理提出了明确的要求和规定。

可靠性信息库是可靠性数据和信息的数据库,是用电子形式存储、处理可靠性数据和信息,并加以利用的一种方式。

国外的工业发达国家都先后建立了数据交换中心,把来自工厂、用户、试验认证机构的各种数据迅速地进行汇总、分类、统计分析,尽可能作成二次情报,以刊物、卡片、手册、缩微胶卷及计算机远程终端联机检索等各种形式实施交换或随时提供咨询服务。最早建立可靠性数据交换中心的是美国,后来欧洲一些国家及日本都先后建立了可靠性数据交换中心。

我国自 20 世纪 80 年代以来,在武器装备研制、生产的主要工业部门、使用部门都分别或共同建立了不同形式的信息管理组织,各单位、部门根据工程项目的需要,建立了质量与可靠性信息体系,积极开展信息的收集、处理、分析、反馈和应用工作,取得了显著的效果。如原国防科工委领导组建的“中国军用电子产品质量与可靠性信息交换网”(简称“国家网”),其“秘书处”和“信息中心”挂靠在原信息产业部第五研究所。“国家网”的宗旨是收集、分析、储存、反馈和交换军用电子产品质量与可靠性信息,研究、开发、推广应用可靠性工程技术及工具,为现役电子武器装备全寿命周期的质量与可靠性管理提供技术支持和信息服务。

收集并建立可靠性数据库系统,可实现数据的信息共享,使信息交换统一、规范化,同时还可使上级主管部门、工程主管部门、承制单位,能准确及时地掌握电子武器装备研制、生产过程质量控制情况、可靠性考核情况、故障(失效)报告、纠正措施落实情况、产品的现场使用情况等。

可靠性数据的收集与分析需要通过严密的可靠性信息系统来管理与控制。由于可靠性数据大量存在于各项可靠性研究、试验及现场使用中,因而只有对其实施有计划、有组织的管理,才能保证数据收集的完整、准确及分析工作的有效。可靠性信息系统,包括可靠性数据的收集系统和数据分析系统,它们负责对各种可靠性数据的收集和汇总,并对其进行定期或适时的分析,以满足各项可靠性技术和管理部门的决策需要。

7.3 可靠性数据收集与分析的基本要求

由于可靠性数据具有随机性、时间性、有价值性、时效性和可追溯性等特性,为了在产品寿命周期内有效地利用数据,包括为改进产品的设计、生产提供信

息，为管理提供决策依据，为保证产品的质量和提高产品的可靠性服务等，确定可靠性收据收集的目的和要求，并依据确定的不同目的及要求来收集相应的数据是很重要的。

7.3.1 可靠性数据收集的目的

可靠性数据收集的目的，大体有如下几方面：

- 根据可靠性数据提供的信息，改进产品的设计，制造工艺，提高产品的固有可靠度，并为新技术的研究，新产品的研制提供信息。
- 根据现场使用提供的数据，改进产品的维修性，使产品结构合理，维修方便，提高产品的使用可用度。
- 根据可靠性数据预测系统的可靠性与维修性，开展系统的可靠性设计和维修性设计。
- 根据可靠性数据进行产品的可靠性分析及可靠性的评估，实施产品改进，实现可靠性提升。

不同类型的组织收集可信性数据的动机是不一样的。可以从人们所处的不同角色视角，分析可靠性数据收集的主要用途。对所有用户而言，对产品可靠性的要求和期望可以归纳如下：

- 寿命。
- 可用性。
- 售后服务。
- 购买成本。
- 使用可靠性。

而专业用户感兴趣的是：

- 确认要购买产品的需求得到满足。
- 最佳的备件库存。
- 最佳的维修。
- 最佳的综合保障。
- 产品可靠性研究。
- 产品可用性研究。

从制造商的角度来看，以下事项是重要的：

- 与市场上相似产品的比较。

- 作为改进下一代产品的基础。

可靠性数据收集的首要目的,是为了改进相关产品及其研制过程。数据的收集加上适当的分析,构成了市场营销、设计、生产及服务的信息闭环。其次是为使生产风险最小化、成本最优化,或者验证与需求的一致性。数据收集应有针对性:为使数据分析可行,要注重对产品工作和失效情况的不断深入了解,并将得到的这些信息应用于一个具体目标。一旦进一步的数据分析及其信息的应用离开了具体的目标,数据收集就会变得无目的性,从而会忽略重要的数据、滥用数据,或将时间和资源浪费在一些无利用价值的的数据上。

7.3.2 可靠性数据收集的要求及注意事项

科研工作需要开展大量的试验。一般说来,试验的观察结果总是受当时当地条件的限制,得到的结果总具有一定的随机性,同样的事件,其试验结果可能因时间地点的不同而不尽一致。因此,如何对试验结果进行去伪存真的分析处理,以便更好地指导今后的设计和试验,是科研工作的重要内容。我们所需要的数据,应该是能够反映客观事实的、准确可靠的数据。那些不反映实际情况的虚伪数据,将会导致错误的结论和行动。因此收集可靠性数据时需要层层把关,才能保证数据的准确性。影响可靠性数据准确性的因素很多,归纳起来,有以下4点,即:原始数据的真实性、数据来源的信息量、统计分析方法的合理性和连续性。

1. 原始数据的真实性

要保证可靠性数据的准确性,首先要保证原始数据的真实性。可靠性的原始数据一般是观察现场或通过可靠性试验而获得的,试验观测的取样方式、试验方案、试验设计能否反映客观实际的真实面貌,对原始数据的真实性有着直接的影响,因此从试验设计一开始,就要牢牢地把好数据真实性这一关。可靠性试验设计包括了产品的环境设计和统计设计。产品的环境设计要尽可能客观地反映真实的工作条件,特别要注意试验应力的选取。产品的统计设计又包含有投试样品数的选取,以及试验测试周期和试验截止时间的确定等问题,因此在产品的试验设计阶段就必须利用抽样理论以及产品的寿命分布等可靠性知识对产品的试验技术进行认真的考虑。

数据的真实性与试验设备及其测试仪表的精度也有极为密切的关系。试验测试中的随机误差是正常的,但系统性误差应该尽量避免,过失误差更是不能允许的。如果由于操作不当或粗枝大叶造成了过失误差,必须重新认真操作加以消除。如果由于仪器结构不良或周围环境改变造成了系统性误差,必须校正仪器重新进行测

量。如果观察的系统性误差小，则称观测的系统的准确度高，此时可使用更精确的仪器来提高观测的准确度。如果观测的随机误差小，则称观测的精密度高，此时可增加观测次数取其平均值来提高观测的精密度。

2. 原始数据的信息量

可靠性指标是一些统计指标。只有在进行大量调查研究并取得了丰富的数据资料的基础上，才能对产品的可靠性水平做出正确的评价。随机事件出现的概率，是随机事件在多次独立观测试验中出现的可能性大小的一种估量，但在有限次的试验中，某一事件的出现次数可能与它的概率值相差甚远。在掷骰子的随机事件中，某一点向上的可能性是 $1/6$ ，但这并不是说，在六次掷骰子的随机事件中，某一点一定要向上一次，很可能在最初的若干次事件中，某一点一次也不出现。因此要正确地评价产品的可靠性水平，必须对产品进行大量的统计试验或长期观测，只有在数据达到一定的信息量后，才能得到准确可靠的产品寿命结论。

3. 统计分析方法的合理性

要想获得准确可靠的数据，必须要有合理的统计分析方法。一般来说，从现场所取得的试验观测值，只是产品整体中的个别样本值。要想从有限个体的观测值去推断总体的统计特征值，就必须要有合理的数据处理方法及统计分析手段，因此数据处理的合理性及其统计分析的置信度是关系到数据准确性的重要问题。同一产品选取不同的样品进行试验，将会得到不同的数据；同一试验数据，采取不同的分析处理，亦会得到不同的结果；同一数据、同一方法，不同的人去处理也有可能得出不同精度的结论。如何分析研究和解决这些差异之间所造成的矛盾呢？这正是统计分析所要研究的问题。总之，可靠性数据处理及其统计分析是一门专门的技术，它要求从事这项工作的人员要有清晰的可靠性概念，以及较好的概率统计知识。

4. 连续性

可靠性数据有可追溯性的特点，随着时间的推移，它反映了产品可靠性的趋势，因此为了保证数据具有可追溯性，要求数据的记录连续。其中最主要的是产品在工作过程中所有事件发生时的时间记录及对所经历过程的描述，如产品开始工作、发生故障、中止工作的时间，以及对其中发生故障时的状况、返厂修理、经过纠正或报废等情况的描述。在对产品实行可靠性监控和信息的闭环管理时，连续性是对数据的基本要求。

综上所述，不难看出数据的真实性与试验的方案设计、技术措施及其设备条件有关，数据的准确性与数据的处理方法及其统计分析技术有关，因此只有试验设计、试验测试以及数据处理人员层层把关，各个部门加强责任感，才能保证数据的准确度。

7.3.3 可靠性数据分析的目的和任务

可靠性分析主要是对产品的故障（或失效）进行分析，产品故障既有因其硬件的缺陷和性能恶化所引起的，也有因软件错误引起的，此外，还有人为原因所致。故障分析就是要找出故障（失效）时的故障模式，分析其故障原因、失效机理，估计该故障对产品及其所属系统可能造成的影响，以及寻求改善措施。可靠性数据分析的基础是可靠性数据，其目的和任务是根据可靠性工作的需要而提出的。一般而言，在产品寿命周期的各阶段，可靠性数据分析的目的和任务包括：

- 在研制阶段进行可靠性增长试验时，应根据试验结果对参数进行评估，分析产品的故障（失效）原因，找出薄弱环节，提出改进措施，以求产品可靠性得到逐步增长。
- 研制阶段结束进入生产前，应根据可靠性鉴定试验的结果，评估其可靠性水平是否达到设计的要求，为生产决策提供管理信息。在投入批生产后又应根据验收试验的数据评估可靠性，检验其生产工艺水平能否保证产品所要求的可靠性。
- 在投入使用的早期，应特别注意使用现场可靠性数据的收集，及时进行分析与评估，找出产品的早期故障及其主要原因，进行改进或加强质量管理，加强可靠性筛选，可大大降低产品的早期故障率，提高产品的可靠性。使用期中应定期对产品进行可靠性分析和评估，对可靠性低下的产品进行改进，使之达到设计所要求的指标。

7.3.4 可靠性数据分析的要求和注意事项

在进行可靠性数据分析时，应考虑其主次性。

主次分析是用统计的方法找出对所分析对象影响最大的因素。对要分析的产品而言，主次分析可从几个方面进行，如对故障频数、故障原因、故障后果、责任、发现时机等。如果分析对象为某产品的故障发生频数，则分析的因素可为组成产品的各系统，将其按主次排列，可找出故障最多的系统；再以系统为对象，仍按故障频数进行主次分析，可找出故障最多的分系统，以此逐级分析，直至找出故障频数最多的设备或单元，即可得到该产品薄弱环节之所在。通过主次分析，也可得到影响产品故障的主要原因及责任等。另外，为综合评价产品中关键系统或设备，除用频数分析外，还可将故障影响后果与发生频数综合在一起，得到主次分析结果，这样得到的关键系统或设备可能故障频数并非最高，但造成的影响却很大。这更有利于对关键系统或设备实施有针对性的分析和改进。



7.4 可靠性数据收集

7.4.1 可靠性数据的分类

可靠性数据主要来源于和贯穿于产品设计、制造、试验、使用、维护的整个过程，例如研制阶段的可靠性试验、可靠性评审报告；生产阶段的可靠性验收试验、制造、装配、检验记录，元器件、原材料的筛选与验收记录，返修记录；使用中的故障（失效）数据、维护、修理记录及退役、报废记录等，所以，产品寿命周期各阶段的一切可靠性活动都是可靠性数据的产生源。总体来说，可靠性数据主要来自实验室的可靠性试验和产品的实际使用现场。从实验室得到的数据称为试验数据，而现场得到的数据则称为现场数据。这两种数据是评估产品寿命各阶段可靠性的重要依据。由于数据产生的条件不同，它们各具特色，故所用数据收集、处理分析的方法也不同。

1. 试验数据

试验数据主要在产品的研制阶段和生产阶段获取。试验数据来自可靠性试验、寿命试验或加速寿命试验，也可来自如功能试验、环境试验、定期试验或综合试验等。可靠性试验主要以截尾试验为主，它们分为定数截尾试验、定时截尾试验和随机截尾试验。在试验中，参加试验的产品如果全部都发生故障（失效），则可称其为完全寿命试验。

在定数截尾和定时截尾试验中，根据样品有无替换又分为：有替换定数/定时截尾试验、无替换定数/定时截尾试验四种。

（1）定数截尾试验

试验前规定产品的故障（失效）数 r ，试验进行到故障（失效）数达到规定故障（失效）数 r 就终止试验。若试验进行中，产品故障（失效）一个就用一个好的样品替换上去继续试验到达规定故障（失效）数终止，这就是有替换定数截尾试验，试验自始至终保持样品数不变。若试验中将故障（失效）的样品撤下不再补充，而将残存的样品继续试验到规定的故障（失效）数 r 才停止，这就是无替换定数截尾试验。

（2）定时截尾试验

试验前规定产品的试验时间 t_0 ，试验进行到规定的试验时间 t_0 时就终止试验。试验分为有替换定时截尾试验和无替换定时截尾试验。

通过可靠性试验获得产品的故障（失效）数据，即可分析、评估产品的可靠性参数。为使评估结果尽量准确，最好在整个试验中采用自动监测方式，进行连续测试，以得到确切的故障（失效）时间，避免在最后的分析中引进较大误差。但是，连续测试不仅在技术上要求高，而且费用也贵，甚至做不到，因此不得不采取间隔测试的办法。测试的间隔时间可以相等，也可以不等，其长短与产品的寿命分布形式有关，如果是指数分布，则开始测试时间短，然后加长，如为正态分布则开始很长，以后缩短，主要目的是不要将故障（失效）过于集中在少数几个测试间隔内。

2. 现场数据

从产品实际使用中得到的数据为现场数据，其中记录产品开始工作至故障（失效）的时间（故障时间），以及开始工作至统计之时尚未故障（失效）的工作时间（无故障工作时间）的数据，是用来评估使用可靠性参数的重要数据，应特别注意收集。现场数据是极其珍贵的，它反映了产品在实际使用环境和维护条件下的情况，相比实验室的模拟条件更代表了产品的表现。美国的一些厂家认为：“内场（或厂内）试验需要做，但无论如何也不可能完全复现真实使用条件，同时对有些可靠性指标来说，如 MTBF，靠外场（或厂外）试验则费用和时间花费太多”。但由于使用地区、环境条件等的差异，相同的产品其可靠性可能不同，所以现场数据波动大，处理时必须按不同情况和处理要求进行分类。以航空产品为例，同样一个机种在空、海军中的使用情况就不一样，其中腐蚀、盐雾、侵蚀等影响就大不相同。

在现场数据中，产品投入使用的时间不同，观测者记录数据时除故障（失效）时间外还有一些产品统计之时仍在完好地工作，以及使用中途会因某种原因而将产品转移至其他地方等，形成了现场数据随机截尾的特性。这是一种随机截尾试验，即在产品进行可靠性试验时，由于某种原因一些产品中途撤离了试验，未做到寿终，现场得到的这些数据可用图 7-2 表示。

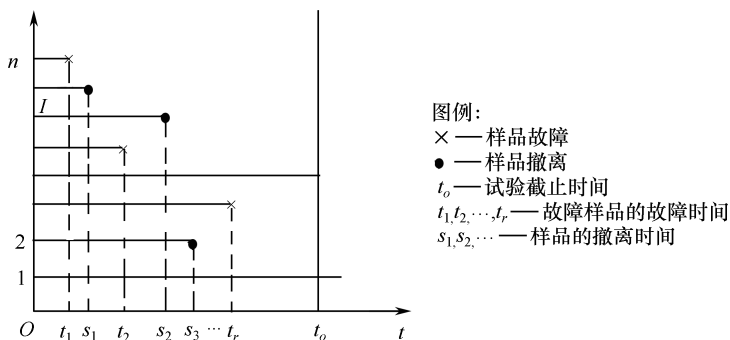


图 7-2 现场试验数据示意图

其中包括了一些产品的故障（失效）时间和另一些产品的无故障（失效）工作时间，即删除样品的撤离时间。

在现场数据中，需要注意对产品实际工作时间的记录，很多产品在使用中无法记录其实际工作时间，只知其工作的日历时间，如测试仪表。对于飞机上安装的设备，一般只记录飞机的飞行时间，但有些设备在飞机上并不是一直都在工作，如启动发电机、应急系统等，这就存在一个实际工作时间和记录时间之比值的问题，通常称之为运行比（或占空比）。运行比可等于 1（持续工作时），也可小于 1（间歇工作时）。然而，对于某些产品，其故障（失效）特性与日历时间密切相关，如非金属产品、橡胶件的老化、腐蚀等，实际工作时间并非主要，对这些产品的记录还应以日历时间为主。

7.4.2 可靠性数据的内容

1. 数据内容概述

一般而言，可以收集的产品及其与可靠性相关的数据包括：

- 产品资料——包含现场使用产品的信息，产品配置及其组成。
- 使用数据——包含产品何时投入使用、现场工作情况，以及什么时候退役（报废）的信息。
- 环境数据——包含产品的工作条件信息，通常它们被认为是影响产品可靠性的重要因素。
- 事件——包含产品寿命期内发生的所有情况信息，包括失效、修理、升级等。

通常，对于一个特定的可靠性工作任务，想获得所有需要的数据是不可能的，这也许是因为运作方面的问题，或是收集数据的成本太高。在这种情况下，通常需要评估为什么需要收集这些数据，并在需要这些数据的理由与收集这些数据的难度之间进行权衡分析。有时，收集这些数据意味着改变组织内部现有的操作流程，在这种情况下，由数据收集进行的可靠性分析所得到的利益必须足以补偿数据收集的困难和费用。

可靠性数据的来源可以是多方面的，其收集方式也有多种。

统计模型总是用某些近似值进行数据建模。应利用工程判断和拟合优度检验来评估近似值是否给出了有用的结果。预处理的灵敏性可以用数据模拟来评价，例如，使用蒙特卡洛法。

2. 产品资料

产品资料通常记录产品的原始制造状态、生产厂商、批次号、状态更改、维修

历史及其他的信总。这些数据在评估各种事件的敏感性因素时特别重要。没有这些信总，可靠性分析将不能确定某些方面相同的特定产品组的趋势。

很多与个别产品相关的事件（例如失效）是产品固有的，它们是由制造瑕疵或设计缺陷引入的。随着产品投入使用（寿命耗损），这些事件被激发（包括零寿命：初始启动失效）。寿命耗损会在单个产品独自累积，因此，如果对关心的产品在其每条数据记录里用某些唯一的序列编号进行标识，就可以对其进行全寿命分析。有些形式的寿命分析没有这样的要求，例如：GB/T 5080.6 的 $M(t)$ （时间 t 的平均累计故障数）分析。

因此，有必要收集母体中所有带有风险的产品信息。母体信息可以从产品资料信息中得到。信息收集通常采用“现场时间”记录。“现场时间”可以指工作时间、日历时间、周期数、里程数和拷贝次数等。

有时对产品整个母体进行信息收集是不可能的，甚至是不适当的，所以，可以利用抽样技术约束数据需求。

3. 使用数据

使用数据是在为用户服务的过程中对一个产品或系统各项功能需求的度量，包括使用时间和频度。为了最大限度地利用收集到的产品使用数据，使进一步的分析能适用于类似的应用而非仅局限在特定的应用范围，需要仔细考虑合适的测试数据。使用数据一般以事件、状态发生和持续时间的形式，采用统计意义和相关风险来表示现场用户的需求，这在产品或系统的鉴定和验证活动中是有用的。

使用数据在一段持续的时间内可能是固定的，也可能是变化的，或者是时而固定，时而变化。

如果设备在 100% 的时间内一直开机，那么使用时间很容易计算，但如果是两台设备，一台连续工作而另一台偶尔工作（称为备份），这样就很难估算该类设备的平均使用时间。通常，想要获得任何一个单台设备的使用时间是不可能的，所以有必要获得该类型设备的平均使用时间。使用信息收集的问题还跟被考查的设备性质有关，这就像一个电话交换机的终端用户会告诉你它的平均使用时间，而一个军事通信设备的用户却不太可能这样做。

使用数据是非常重要的，因为进一步的分析可能要在这些保存的数据上进行，因此，分析结果会被淹没在大量不准确的使用数据里。很多设备都装有使用时间指示器，用来监测该设备的实际使用时间。但这也存在问题，有时只能给出粗略的实际使用时间。

使用数据并非只基于时间，也可能基于运行或循环（如产品的使用次数）。

4. 环境

同样，环境对产品或系统的寿命有着破坏性的影响，因此，环境应力的持续时

间和强度必须包含在产品或系统的鉴定活动中。为了恰当地定义现场使用要求，对元器件使用环境的测量应明确输入环境和元器件对这些环境的响应。这些要求为应用等效的加速试验来验证产品、满足可靠性要求提供了基线。

一个比较恶劣的环境能更快地引起事件的发生。一个特定的事件通常与环境的多方面相关，根据分析的需要，可能需要全部记录。环境测量的位置也是重要的，例如，飞机舱内和发动机上的环境就差别很大。

一个与使用相关的环境因素是开机和关机所带来的损害。依据设备类型，这种开机/关机的应力可能比稳定状态下的环境条件更重要、更有意义。

5. 事件

事件可能包括失效、维修活动等。失效事件可以包括系统失效、从属失效、冗余系统失效、没有造成系统失效的失效及潜在失效。在已发布的相关标准涉及的众多可靠性技术中，最为重要的事件是失效。

在期望获得与故障维修有关的资源和费用信息的同时，还必须记录维修信息，以便有足够的信息确认该修理，为分析提供支持。事实上，应注意的是，一次对当前失效的修复活动可能会成为下一个失效的原因，所以，维修信息是进行详细可靠性分析的重要信息来源。

在对事件进行任何进一步的数据分析之前，将事件按类别分组是必要的，这对执行分析的人员也是有意义的。例如，一个复杂电子系统的失效事件可以按设计、制造、供应、维护、损坏、软件 and 没有发现失效来分类。有时，对事件的分类可以在更低的层次进行，这取决于可用的数据和研究的关注点。例如，可能会给出元器件类型、相关位置及失效模式。

事件的分析过程始于对事件的明确分类，以及失效或使用特性现场数据收集的目的。

对于失效事件，分析首先是对失效的确认。如果没有发现失效，可以直接归入“没有发现失效类别”。当一个失效被确认，就可以开始详细的失效分析，以隔离实际的失效模式和引起失效的机理。

对于使用特性，需要确保收集了恰当类型的数据。这可以通过数据需求和在开始数据测量程序前完成的计划分析来实现。数据收集方案和装置应能直接为分析提供有用的数据并转化为使用信息。

对于软件，失效通常是间歇性的（软错误），或许重新运行即可排除。在这种情况下，用户使用软件的意图和实际操作可能会在事件分类时引起关注。

6. 数据来源

尽管可靠性数据的可利用性及其利用已涉及了不同的产品类型和组织，但仍然

有很多其他可靠性数据来源，因此，要列出所有的数据来源几乎是不可能的。

直接信息是指通过产品制造商收集的信息。间接信息是指从销售和维修等获得产品信息的第三方收集的信息。直接和间接信息的相对划分取决于产品类型。一般而言，专业类产品（如：通信开关，工厂设备）的信息收集绝大多数是直接的，而消费类产品（如：家电产品，移动电话）一般都是间接的。通常，人们更喜欢直接信息，因为采用正确的数据收集程序可以保证这些数据的质量，而从第三方来的信息，其质量通常是未知的。

现场产品的类型及其母体大小可来自销售、调度、定购、发送和安装记录。通常，所有这些类型对特定的产品来说都是有用的，有助于建立一张完整的产品分布图等。有时，也可通过回收的产品保修凭证了解产品/软件的安装位置和开始使用日期。

产品信息包含诸如产品的内部结构信息，例如，使用了哪些线路板、模块、元器件等。这类信息通常包含在产品的工作卡或类似材料里。服务记录、保修记录、修理的产品记录和已经使用的备件经常可以给出关于哪些实际的产品失效了，以及在什么情况下失效的有用信息。

报废记录提供产品是何时退役的，不应再作为用于分析目的的母体的一部分。客户的投诉也可以用来识别一个特定产品的所在地，还可能提供有关的失效信息，特别是那些间歇的失效信息，也可以利用用户的报告和意见帮助完成一个数据集。当保险索赔及其范围记录可以利用时，可以用来识别一个产品的位置和使用情况。如果保修卡是随着产品而发出的，使得购买者或使用者在购买产品或开始使用时可返回保修卡，这样就可获得有用的信息。在很多销售部门，这是获取这些信息的唯一途径。

有时候，产品被设置成开始投入服务时就自动通知制造方。这类产品典型的有通信设备，或者与通信系统相连，同样可以向制造者报告其使用和健康状况的其他产品。如果产品不报告信息，就可以推测该产品可能不再被使用了。为此，对于较昂贵的设备，或许可以单独添加一个通信功能。

7.4.3 可靠性数据收集的原理

1. 基于时间的数据收集

基于时间的数据收集有连续的和间断的。基于时间的数据收集方法有以下几种：

- 连续的数据收集。
- 窗口式数据收集。
- 多窗口式数据收集。
- 滚动窗口式数据收集。

连续的数据收集是指贯穿产品整个寿命周期，持续地积累数据，见图 7-3。

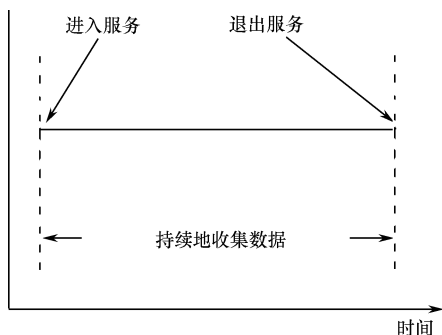


图 7-3 连续数据收集

窗口式数据收集是指在产品寿命周期的一个时间窗口中收集数据，见图 7-4。

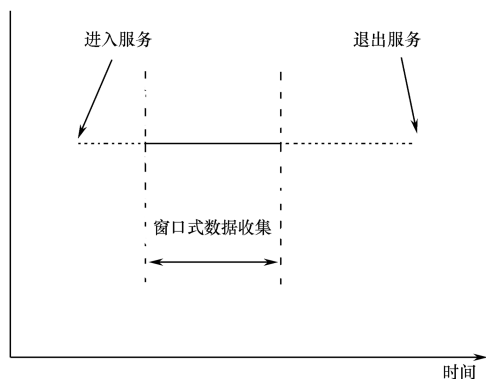


图 7-4 窗口式数据收集

多窗口式数据收集是指在产品寿命期内从多个时间窗口中收集数据，见图 7-5。

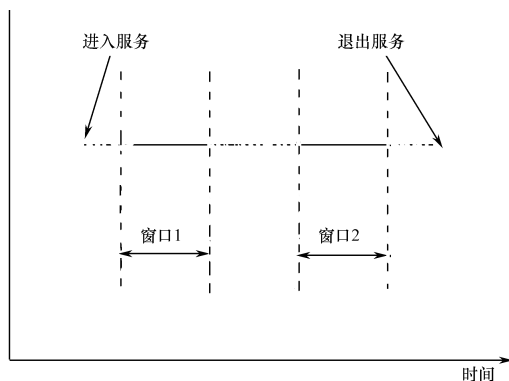


图 7-5 多窗口式数据收集

滚动式窗口数据收集除了窗口的开始时刻和结束时刻随时间滚动外，都与窗口式数据收集类似。这就意味着收集新数据的同时总是丢弃最旧的数据。丢弃旧的数据是为了面对这样的事实——产品确实过时了，其数据不再具有代表性，或是为了保持数据采集系统的内存空间。应丢弃与关注的事件无关的数据，只有这样，当一个事件发生时，才能记录更多的事件及其背景。利用窗口数据可得到整个工作期间的平均值，这可以通过短时间的数据收集并假设整个工作期间的观测值是相同的来实现。

应当注意数据收集的时间尺度可能不用日历时间，而用其他的时间尺度方式。这些时间尺度可能是“工作时间”——系统工作的时间，或者是“加电时间”——系统加电的时间（包括待机和运行）等。还有，时间尺度可能根本不是以时间为基础，可能是基于运行或工作循环的（如汽车的驾驶次数或里程数）。这些时间尺度之间通常有联系，如图 7-6 所示，采用工作/日历时间表示。

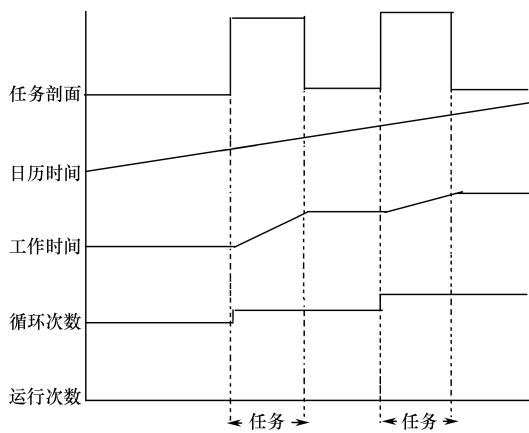


图 7-6 各种时间尺度

在图 7-6 顶端的曲线给出了一个典型的任务剖面，可以看到，日历时间在整个剖面上一直都在增长，而工作时间只是在剖面的工作部分才增长；循环次数只在每个任务的开始处增加（也可以选择剖面的结束处增加循环次数）；运行次数的增长只发生在任务执行阶段。

2. 完整的和有限的数据收集

完整的数据收集是指对现场使用产品的每种情况都进行数据收集；有限的数据收集将收集范围限定在上述情况的一个子集上。例如，在特定区域或特定用户使用的所有产品。有限的数据收集可以使用多种抽样方法来决定被跟踪产品的区域及其数量。

通常，要获得大量生产的消费类产品的信息，唯一的途径是在规定的市场上投放一批产品，记录产品的使用时间以及失效次数。同样,也可以将市场信息反馈限定于特定的市场或特定的用户，并将精力集中在来自他们的市场反馈上。这有助于减



少资源的使用，或通过更好地与有关营销部门协作，提高反馈数据的质量。

该技术是抽样的一种方式，这样的抽样技术是常用的。为了从一组数据中得到大量的信息，有必要仔细选择数据收集方法，以及分析这些数据所采用的方法——并将两者一同考虑。通常是先收集数据且仅当收集完成后才考虑数据分析程序，这是一种非常错误的方法。一开始就应确定需要收集什么信息。

抽样的主要目的是根据由母体抽取的样本确定需要的信息，或有关母体尽可能多的信息。

(1) 母体类型

母体可以方便地分类如下：

- 有限存在的母体，如仓库中储存的产品（来自给定的生产线）或者树上的苹果。从这样的母体中抽样可能是随机的但不能称为简单的，因为这样连续抽取是不独立的。通过每次从母体中抽取个体后再放回，就可以将其转变为简单抽样程序。
- 无限的母体，如从用数学方法生成的数字序列中选取数字。应注意的是，用放回的方法从有限存在的母体中抽样，可以看成是从无限母体中抽样，因为这种抽样过程永远不会把母体耗尽。
- 假定的母体，如通过掷骰子得到的数字序列。这种连续的掷就构成了从一个并不存在的母体中抽取现实数字的抽样过程。

值得关注的是，在很多情况下，母体中的个体是用两种（有时更多）互斥的特征描述的，如：“工作或失效”；“好的或坏的”；“有利的或不利的”；“完好的，性能丧失或灾难性故障”等；这类母体中的个体被认为是具有特征的，针对这类母体的抽样被称为特征抽样。而在有的情况下，母体中的个体是依据连续的可测量的特征来区分彼此，如：重量、故障时间、成本等，即连续母体，这样的抽样程序被称为变量抽样。

(2) 随机抽样

随机抽样是用这样的方式选取样本的，即每个可能的样本都有一个可计算的选中概率。而事实上是没有必要计算这一概率的，因为抽样程序的规范和控制全都需要应用概率论。

- 简单随机抽样——如果一个随机抽样程序使每个可能的样本都有同等的选中概率，并且连续抽取是独立的，那么这种程序被称为简单随机抽样。
- 分层抽样——另一种非常实用的抽样程序是分层随机抽样，它在某些方面优于简单随机抽样。实质上，该抽样程序是在对母体分层的基础上再对每层进行子抽样。在每层中母体的每个个体和该层中其他个体一样，在子抽样中具

有相同的出现机会。这种抽样方法的效果是使样本更均匀地散布在母体当中，同时在每层里保持了随机性原理。

(3) 样本容量

当对应的母体大小可能为几万，几十万时，可以从小到几百的样本容量中得到有用的信息。看来要得到有意义的结果，样本容量应与母体大小成相应的比例，这似乎符合逻辑，其实并不是这样。样本所含的信息量和有效性主要与样本的绝对数量和随机程度有关。

(4) 抽样误差

假设在一个随机抽样程序中，从母体中抽取规定数量的样本。任何两个样本反映出完全相同的母体信息是极不可能的。其中一个原因是：母体中的个体之间存在一些差异，以至与其他样本相比，一个样本可能会随机地包含不同数量的特定属性的个体。但是，如果所有母体中的个体相互之间的差异非常小，只用少量个体组成样本，就可以很好地包含所有想要知道的母体信息。特别地，如果所有的个体都是相同的（个体零差异），只需一个个体组成样本就足够了。因此，造成抽样误差的一个原因是母体中个体之间的差异。

当通过计算样本均值来比较样本时，另一个会遇到的差异来源于与实际的样本容量有关。如果每个样本（确定的）数量是庞大的，则样本均值之间的差异，会比小样本量的小一些。

偏差可认为是某些参数的系统性背景差异，偏差影响到测试结果。比如，长期从母体中抽取连续的样本，其间可能刚好出现了一些对获取样本的测试结果构成直接影响的情况，诸如温度变化、压力变化，或人员疲劳和精神不集中。这样的影响结果称为偏差。偏差影响获得测试结果真实值，并且有时很难避免。

3. 定量和定性数据收集

定量数据收集是收集可以用数值表述的情况，例如一个数字。而定性数据收集是收集“软性”的信息，例如事件发生的原因。这两类数据都是重要并相互支持的。数据收集的类型取决于用该数据来回答问题的种类。

4. 数据集中的数据删失

对事件发生的确切时间而言含有不确定性的现场数据称为删失（censor）数据。删失意味着将给定持续时间后或给定事件数以后所获得的数据排除在某一特定评估以外。对删失数据统计处理的方法取决于表现出来的删失类型。注意，“删失”一词在一些文献（尤其是早期的文献）中也称为“截尾”。

“完整数据”也就是观测或知晓每个产品的寿命时间值。例如，用于寿命数据

分析的数据，如果说是“完整的”（这在现场数据收集时并不多见），则应包含现场所有单元的故障前时间。

通常，在分析寿命数据时，所有的单元可能未必都已历经受关注的事件，或者不知道事件发生的时间，这类数据就是删失数据。有 3 种可能的删失方案：右侧删失数据（也称为延迟数据）、区间删失数据和左侧删失数据。

（1）右侧删失数据

右侧删失（延迟）数据是最普遍的情况（见图 7-7）。在现场的 5 个单元中只有 3 个在分析时段历经了事件（用黑色方块表示），对于两个还未历经事件的单元（带箭头的直线）就是延迟数据（右侧删失数据）。术语“右侧删失”意味着受关注的事件发生在分析点的右侧。

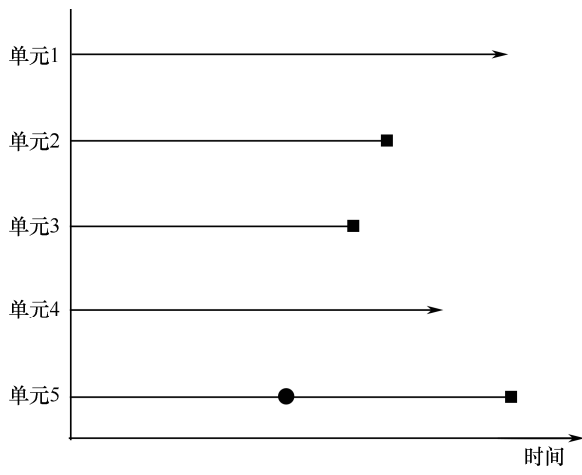


图 7-7 右侧删失（延迟）数据

（2）区间删失数据

区间删失数据是指事件发生在某一区间内，但其确切发生时间不确定。这可能是由于对系统的观察不是连续的，而是偶尔观测。例如，启用 5 个单元，并每隔 100h 观测一次，可以得到的唯一信息是：事件发生在某个确定时间区间内（在图 7-8 中圆圈之间的某个时刻，方块表示事件发生前最后的已知工作状态）。

（3）左侧删失数据

左侧删失数据与区间删失类似（见图 7-9），其只知道一个事件的发生时间在某特定时间之前，如图 7-9 所示用向左的箭头表示。

在 GB/T 5080.1 中可以找到更多关于数据删失及其对统计分析的影响的信息，这里不再赘述。

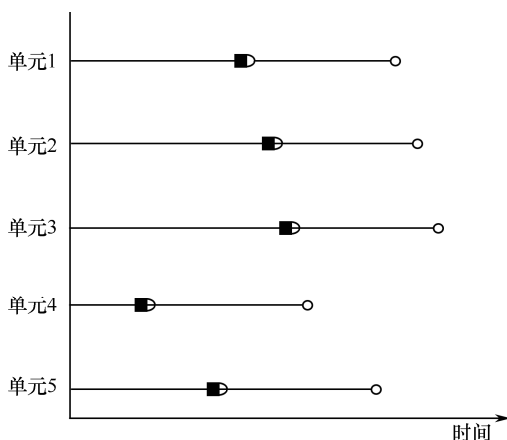


图 7-8 区间删失数据

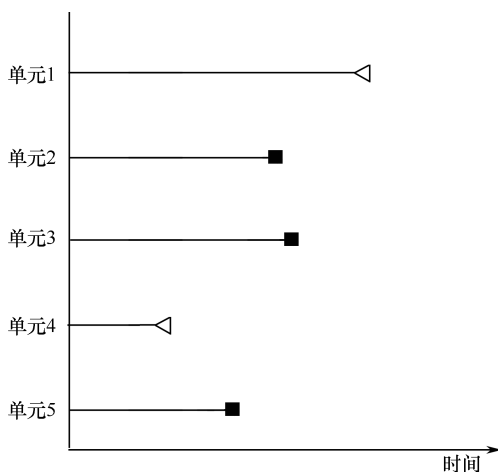


图 7-9 左侧删失数据

7.4.4 可靠性数据收集的方式

现场数据收集的方式一般有 3 种：一是对现场工作人员分发表，令其逐项填写，然后定期回收；二是培训一批专业人员、编制调查纲目，有计划、有目的地深入现场进行调查，收集重要的可靠性数据，然后整理成统一的格式；三是开发可靠性数据自动收集计算机应用系统，自动收集与产品或系统可靠性相关的数据。

数据报表的编制要注意合理性、全面性和方便性。所谓合理性就是要求报表的记载内容尽量反映客观现实，能准确记载产品的工作条件、工作时间及故障情况；所谓全面性就是要尽量利用现场的各种信息，记载的项目尽可能详细；所谓方便性就是要求报表格式便于记载，便于分类查找，便于统计分析，便于制作缩微胶片，



便于进入计算机，便于适应数据库管理系统。

可靠性的数据报表一般应包括如下内容：

- ① 报告号和日期。
- ② 使用者姓名、地址、产品位置。
- ③ 报告性质（如“使用”报告、“失效”报告、“维修”报告等）。
- ④ 产品鉴定。
- ⑤ 调查的产品数。
- ⑥ 产品履历，包括：

- 制造或调机日期。
- 调整情况。
- 首次使用日期。
- 累计工作时间。
- 调整日期。
- 最近使用日期。
- 储存运输条件。
- 最近维修的性质和日期。
- 在良好状态下非工作累计时间。
- 在非良好状态下非工作累计时间。
- 储存累计时间。

- ⑦ 一般工作条件，包括：

- 安装形式，如：
 - ◆ 机动性水平（固定、移动、携带）。
 - ◆ 架设性质（地面、人背、车载、船载、机载、其他）。
- 特殊环境，如：
 - ◆ 室内、露天、棚下、其他。
 - ◆ 温度范围（平均和极限值）。
 - ◆ 湿度。
 - ◆ 气压范围。
 - ◆ 大气性质（空调、温度调节、净化、尘、沙、盐、腐蚀、其他）。
 - ◆ 振动、冲击、碰撞
- 工作方式，如：
 - ◆ 连续。

- ◆ 间歇。
- ◆ 储备。
- ◆ 一次使用。
- ◆ 储存。

⑧ 产品失效说明

- 症状和预兆。
- 在工作中和周期性检查中检出的故障。
- 产品失效模式。
- 失效原因，如：
 - ◆ 内在原因。
 - ◆ 误用。
 - ◆ 由维护工作引起的。
 - ◆ 外部原因。
 - ◆ 二次失效。
 - ◆ 未知。
 - ◆ 不肯定。

⑨ 产品失效分析。

⑩ 处理措施。

⑪ 现场或维修工程师的估计。

⑫ 报告、起草人姓名、签字。

7.4.5 可靠性数据收集的程序和方法

可靠性数据的收集应有周密的计划，但在不可能做到面面俱到的情况下，应根据需求分析选择重点产品和地区作为数据收集点。数据收集的一般程序如下。

1. 进行需求分析

由于不同的寿命阶段对数据的需求是不同的，因此，在进行数据收集以前必须进行需求分析，明确数据收集的内容及目的。

2. 确定数据收集点

在不同的寿命阶段有不同的数据收集点，如在研制、生产阶段，单位内部的试验数据就应选实验室、产品生产检验点、元器件及材料筛选试验点等作为数据收集点；对于现场数据，主要是使用部门的质控室或维修部门等。在选择重点地区或部

门时，以有一定的代表性为好，如使用的产品群体较大，管理较好，使用中代表了典型的环境与使用条件等。对于新投入使用的产品，应尽可能从头开始跟踪记录，以反映其使用的全过程。

3. 制订数据收集表格

数据收集表格是用来系统地收集资料和积累数据，确认事实并对数据进行粗略整理和分析的统计表。制订数据收集表格是进行数据收集前最主要的技术工作，根据需求制订收集数据所需的、规范化的和易于识别的表格，能够促进按统一的方式收集资料，以便于计算机处理，也便于在同行业或同部门内流通；有利于减少重复工作量，提高效率，也有利于明确认识，统一观点。实践证明，表格的统一、规范化是一项极其重要的工作。

以电子产品为例，其可靠性数据收集常用的表格有：

- 电子元器件质量认证试验合格产品信息表
- 电子产品安全认证试验合格产品信息表
- 电子产品集中测试试验信息表
- 电子产品国家监督抽查质量检验（复验）信息表
- 电子元器件失效率试验数据信息表
- 电子元器件累积失效率试验数据表
- 电子元器件寿命试验数据表
- 电子元器件寿命试验原始数据表
- 电子元器件加速寿命试验数据表
- 电子元器件加速寿命试验原始数据表
- 电子元器件可靠性筛选试验数据表
- 电子元器件试验数据统计表
- 电子设备信息表
- 电子设备可靠性试验数据表
- 电子设备现场工作（非工作）可靠性数据统计表－设备部分
- 电子设备现场工作（非工作）可靠性数据统计表－故障部分
- 电子设备现场工作（非工作）可靠性数据统计表－元器件清单
- 电子设备现场工作（非工作）可靠性数据统计表－元器件部分
- 电子元器件储存可靠性数据统计表
- 电子元器件失效模式及失效机理信息表
- 电子产品生产线信息表

由上述表格组成的数据收集系统如图 7-10 所示。

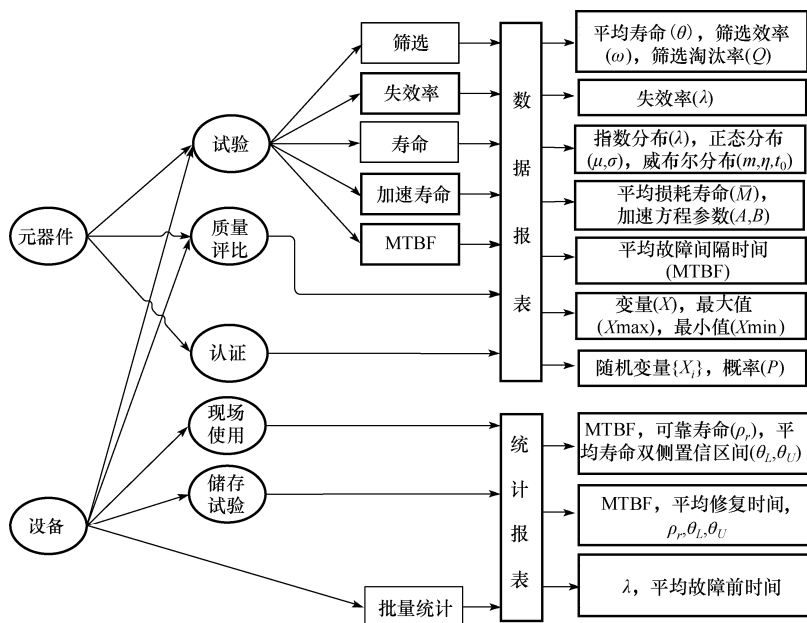


图 7-10 可靠性数据收集系统

4. 数据收集的方法

在建立了完善的数据收集系统以后，数据可依其传送的途径，按正常流通渠道进行，当数据收集系统运行尚不完善时，可用以下两种方式进行：一是在使用现场聘请信息员，让其按所要求收集的内容，逐项填表，定期反馈；另一方式是信息系统派专人下到现场收集，按预先制订好的计划进行。两种方式收集的效果是相同的。

5. 在数据收集应注意的问题

虽然现场数据反映了实际使用中产品的可靠性，但相同产品绝不是都在相同条件下使用，因而数据收集时应区分不同条件和地区，如对腐蚀而言，南、北方差异很大，空中和海上差异很大。同一个仪表在同一产品中由于安装部位不同，所处条件差异也很大，如发动机周围的条件就比仪表舱内恶劣得多。在数据收集时应注意区别。

收集现场数据时，一般是从产品投入使用就开始跟踪记录，直至退役、报废为止。但由于产品的可靠性问题，可能需要进行改进，尤其在投入使用的初期，那么为了评估产品当前的可靠性，在处理数据时，应注意区分，不能将改进前、后的数据混同处理。以某型号飞机为例，在投入使用时，飞机上的六大系统（自动领航仪，航行雷达等），由于故障多，反馈至工厂后，产品进行了改进，之后这些部分的故障明显减少。如果收集数据时，不加说明，分析时不区分这种情况，将其混同

处理，那么结果肯定不能代表产品当前的水平。然而，如果为了分析产品的可靠性增长，从其可靠性增长过程来看，又需分析产品改进前后的可靠性水平，以评估其可靠性增长的状况，因此在对待不同的分析目的时，应分不同的状况来处理。这种情况的考虑可以从产品编号或出厂批次上判别，所以对产品编号和批次的记录是不能忽视的。在现场数据的收集，由于各种因素的影响，数据丢失现象严重，造成数据不完整和不连续，影响了对数据的分析。在收集数据时，应对这些情况进行了解，以便对分析结果的修正或作为对评估方法进行研究时的依据。另外，对于数据收集人为的差错，只能对收集数据的人员进行培训，加强责任心教育，才能逐步避免。

7.5

可靠性数据处理与统计分析概述

在试验或现场使用调查中可以得到大量的观察数据。一般的试验观测值只是产品整体中的个别样本值，而且由于受各种条件的影响，其结果往往具有一定的随机性。为了从有限的个体观测值中去推断总体的统计特征值，就需要有合理的数据处理方法及统计分析手段。如果已经知道产品的失效分布类型及其参数，就可利用可靠性指标间的关系图来计算产品的可靠性指标，因此试验数据统计分析的主要问题，就在于如何根据试验的子样观测值来确定产品的寿命分布类型及其分布参数。

可靠性数据的统计分析方法应视具体情况而定，内容也比较多。以寿命试验的数据处理过程为例，其概要内容如图 7-11 所示，具体的方法将在下面的相关章节中阐述。

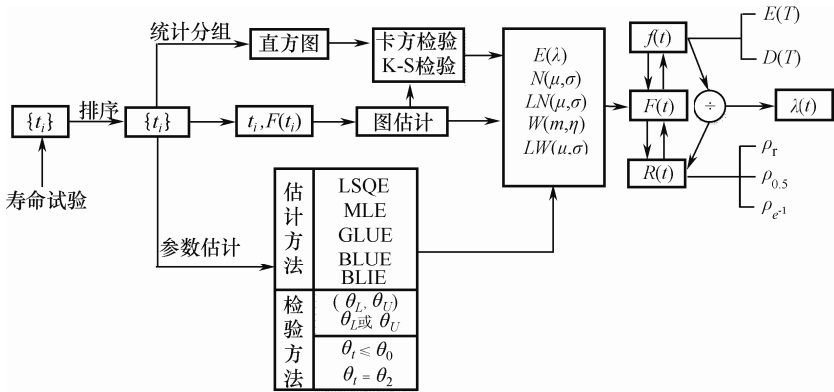


图 7-11 寿命试验数据处理概要图

分析是对计算值、分布和趋势的鉴别和量化。分析可以针对整个产品、单独模块、特定的失效模式、特定的用户、特定的事件、特定的环境等进行。只要选择满足

必要的挑选规则的事件，就能达到分析目标。数据分析不是单纯的计算，而是在对数据的一系列检验，在一系列结构检验中，探测数据的范围和深入特性。数据收集和分析也应随着经验的积累而得到进步和提升。通常，有效的方法是先从主要的方面检验数据，然后以此为引导进行更深入的检验。可靠性数据分析的主要方法有：

- 探索性数据分析——探索性数据分析的目标是为了获得数据的共同特性。
- 事件的数量——最基本层次的分析是统计一个特定时期或内含几个从属时期内的事件数量。事件数量可以适当地划分为若干子类，比如导致紧急停工、用户投诉、安全问题的事件数量，再进一步细分到引起这些问题的模块。检查事件的数量可以识别需要开展进一步调查确认的特定领域。
- 比率——比率是指在单位时间内、每次操作中或每个周期里发生的事件次数。比率的统计可以显示出事件数量是如何随时间变化的。比率可以是恒定的或者非恒定的。
- 分布分析——下一层次的分析是进行分布分析（如：威布尔分布）。有鉴别输入数据符合各种分布的准则，这些准则会在相关标准里描述。
- 非参数分析——如果分布分析不适用，可以使用非参数分析。通常非参数分析的限制比分布分析少，但是获得的信息没有分布分析多。

可靠性数据处理、分析的目的和用途有多方面，为方便读者查阅，笔者将主要的可靠性数据分析用途，以及其数据需求、可参考的技术标准列表，列于表 7-1 中。

表 7-1 可靠性方法的数据需求

序 号	用 途	数据需求	参考标准编号	参考标准名称
1	如何应用寿命周期费用的原理	确定费用要素和项目总费用的成本	IEC 60300-3-3	寿命周期费用计算
2	如何选择和实现风险分析技术	确定事件发生的频率、事件发生可能性和持续时间	IEC 60300-3-9	技术系统的风险分析
3	如何表述元器件和组件的可靠性数据	相关元器件的失效次数，元器件的失效模式，相关元器件的失效前时间	IEC 60319	电子元器件可靠性数据表示法
4	如何估算恒定失效率	产品失效前时间（图形分析程序要求最少有 4 个失效前时间的观测值）	GB/T 5080.4 (IEC 60605-4)	设备可靠性试验；可靠性测定试验的点估计和区间估计方法（指数分布）
5	如何确定失效率是恒定的	每个关联失效的失效前时间（数值分析程序需要最少有 10 个失效前时间观测值；图形分析程序需要最少 4 个失效前时间观测值）	GB/T 5080.6 (IEC 60605-6)	设备可靠性试验；恒定失效率假设的有效性检验

(续表)

序 号	用 途	数据需求	参考标准编号	参考标准名称
6	如何识别早期失效	每个关联失效的失效前时间（数值分析程序需要最少有 10 个失效前时间观测值；图形分析程序需要最少 4 个失效前时间观测值）	GB/T 5080.6 (IEC 60605-6)	设备可靠性试验： 恒定失效率假设的有效性检验
7	如何达到和验证维修目标	维修活动的原因，完成维修活动的类型，维修活动工时和等值日历时间，总的停机时间，工作小时数，维修队伍人员数量和技术水平，使用的测试检查设备和备件消耗	GB/T 9414.6 (IEC 60706-3)	设备维修性导则：第七部分：维修性数据的收集、分析与表示
8	如何使用统计方法进行维修性评估	在指定设备进行维修所需的时间	GB/T 9414.8 (IEC 60706-6)	设备维修性导则：第九部分：维修性评价的统计方法
9	如何确定故障及其后果	事件发生的概率和频率	GB/T 7826 (IEC 60812)	故障模式和效应分析程序
10	如何确定引起不希望事件的条件和因素	事件发生的概率	GB/T 7829 (IEC 61025)	故障树分析程序
11	如何为评估性能设计组件试验	单件可修产品的能工作时间和不能工作时间	GB/T 15647 (IEC 61070)	稳态可用性验证试验方法
12	如何建立一个产品的可靠性框图模型以检验其结构	产品结构描述和每个构成模块的失效率	IEC 61078	可靠性框图方法
13	如何验证失效率的观测值是否遵循给定的要求	关联失效的观测数，累积工作时间或累积关联日历时间	GB/T 5080.7 (IEC 61124)	设备可靠性试验： 恒定失效率假设下的失效率与平均无故障时间的验证试验方案
14	如何验证失效强度的观测值是否遵循给定的要求	关联失效的观测数，累积工作时间或累积关联日历时间	GB/T 5080.7 (IEC 61124)	设备可靠性试验： 恒定失效率假设下的失效率与平均无故障时间的验证试验方案
15	如何验证平均故障前时间（MTTF）的观测值是否遵循给定的要求	关联故障的观测数，累积工作时间或累积关联日历时间	GB/T 5080.7 (IEC 61124)	设备可靠性试验： 恒定失效率假设下的失效率与平均无故障时间的验证试验方案

(续表)

序 号	用 途	数据需求	参考标准编号	参考标准名称
16	如何验证平均故障间隔时间（MTBF）观测值是否遵循给定的要求	关联故障的观测数，累积工作时间或累积关联日历时间	GB/T 5080.7 (IEC 61124)	设备可靠性试验：恒定失效率假设下的失效率与平均无故障时间的验证试验方案
17	如何进行设计评审	复查产品、事件的失效率或失效强度，事件发生的频率，产品的失效模式和机理，以及发生频率	GB/T 7828 (IEC 61160)	可靠性设计评审
18	如何评估一个可修系统的产品成熟度	所有关联失效的数量，每一关联失效的累积关联试验时间	IEC 61164	可靠性增长——统计试验和评估方法
19	如何检验产品的损耗情况	受试产品的数量，每个故障产品的故障前时间	IEC 61649	威布尔分布数据的拟合优度检验，及其置信区间和置信下限
20	如何估计保证期内产品的失效数	受试产品的数量，每个故障产品的故障前时间，最少需要10个观测值	IEC 61649	威布尔分布数据的拟合优度检验，及其置信区间和置信下限
21	如何比较两个失效率，并观察其是否存在统计意义上的差异	关联产品的失效前时间，存在风险的产品数量	IEC 61650	两个恒定失效率和恒定失效（事件）强度的比较程序
22	如何比较两个事件频率或强度，并观察其是否存在统计意义上的差异	关联事件的失效前时间	IEC 61650	两个恒定失效率和恒定失效（事件）强度的比较程序
23	如何转换在不同环境条件下电子元器件的恒定失效率	电子元器件在给定条件下的失效率，电子元器件使用环境的信息	IEC 61709	电子元器件——可靠性——失效率的相关条件，以及用于转换的应力模型
24	如何估计幂律模型的参数	每一关联失效的失效前时间	IEC 61710	幂律模型——拟合优度检验和评估方法

7.6 可靠性数据的初步处理

可靠性数据的初步处理，一般是通过采取一定的手段，对数据进行初步的统计和处理，观察其统计特征量，寻找其中可能隐含的规律。

同一批产品的多次重复性试验或同一批产品的多次观测数据，一般都具有集中性和分散性这两个特点。

7.6.1 数据的集中性和分散性

1. 数据的集中性

多次重复性试验数据，虽然参差不齐，但一般情况下都会密集在某些数点的范围内。数据的这种集中倾向，称为数据的集中性，通常采用算术平均值、几何平均值、中位数以及众数等统计尺度来表征。

(1) 算术平均值

一组数据的和去除以这组数据的个数，得到的商就是这组数据的算术平均值，通常简称为均值。假若有 n 个观测值，分别以 $x_1, x_2, \dots, x_i, \dots, x_n$ 来表示时，则其均值 \bar{X} 为：

$$\bar{X} = \frac{x_1 + x_2 + \dots + x_i + \dots + x_n}{n} = \frac{1}{n} \sum_{i=1}^n x_i \quad (7-1)$$

(2) 几何平均值

若试验观测数据有 n 个，取级联乘积的 n 次方根，就是几何平均值。几何平均值一般可以写成：

$$\bar{X}_g = \sqrt[n]{x_1 \cdot x_2 \cdots x_i \cdots x_n} = \sqrt[n]{\prod_{i=1}^n x_i} \quad (7-2)$$

或：

$$\lg \bar{x}_g = \frac{1}{n} \sum_{i=1}^n \lg x_i \quad (7-3)$$

(3) 中位数

在一组数据中，按其大小排列起来，恰好在中央的数就称为中位数。较中位数大的数据的个数和较中位数小的数据的个数是相等的。若数据的个数为奇数时，中位数就是在中央的数据；若数据的个数为偶数时，在中央的数据便不是一个而是两个了，这时取这两个数的算术平均值为中位数。

(4) 众数

众数是一组数据中个数最多的数据，也就是说众数是在数组中出现频率最高的数。

【例 7-1】 设有 A、B、C、D 四组数据，它们分别为：

- A 组：{6、6、6、6、6、7、7、7、7、8、8、8、9、9、10}
- B 组：{6、7、7、8、8、8、9、9、10}

- C 组: {6、7、7、7、8、8、9、10}
- D 组: {6、7、8、8、9、9、9、10}

不难得到其算术均值、几何均值、中位数以及众数（见表 7-2）。

表 7-2 四组数据的集中性特征量

分 组	算术均值	几何均值	中位数	众 数
A 组	7.333	7.23	7	6
B 组	8.00	7.92	8	8
C 组	7.75	7.66	7.5	7
D 组	8.25	8.16	8.5	9

（5）加权平均值

在具体计算的实践中可以看出，算术平均值的计算有时可以写成：

$$\bar{x} = \frac{1}{\sum_{j=1}^k \gamma_j} \sum_{j=1}^k \gamma_j \cdot x_j = \frac{1}{n} \sum_{j=1}^k \gamma_j \cdot x_j = \sum_{j=1}^k w_j \cdot x_j$$

上式中的 w_j 称为“权”，这种求均值的表达方法称为加权平均。

（6）正斜扭和负斜扭

由例 7-1 可以看出，均值、中位数、众数有时可能是同一个数值，如 B 组数据所示。如果均值大于众数，则称数据具有正斜扭，如 A 组、C 组数据所示。如果均值小于众数，则称数据具有负斜扭，如 D 组数据所示。

2. 数据的分散性

多次重复性试验所得到的一些数据，往往都是参差不齐的。数据参差不齐的这种特性，称为数据的分散性。通常采用极差、方差或标准离差等统计尺度来描述数据的这种分散性。

（1）极差

任何一组试验观测数据总存在最大值和最小值。观测数据的最大值与最小值之差，称为这组数据的极差。一组数据的极差表示了这组数据的变化范围，一般地， n 个观测数据的极差可以表示为：

$$R = \max\{x_i\} - \min\{x_i\} \quad (i=1, 2, \dots, n) \quad (7-4)$$

（2）方差和标准离差

方差和标准离差是表征观测数据与其均值之间的偏离程度的。一组数据中的各个数据与其均值之间的距离的平方和，同这组数据个数的比值，称为这组数据的方差。



假定这组数据的均值为 \bar{x} ，这组数据分别以 $x_1, x_2, \dots, x_i, \dots, x_n$ 表示，则其方差表达式可写为：

$$\sigma_n^2 = \frac{\sum_{i=1}^n (x_i - \bar{x})^2}{n} \quad (7-5)$$

方差的平方根称为这组数据的标准离差，即：

$$\sigma_n = \sqrt{\frac{\sum_{i=1}^n (x_i - \bar{x})^2}{n}} \quad (7-6)$$

如果令

$$\bar{x}^2 = \frac{1}{n} \sum_{i=1}^n x_i^2 - (\bar{x})^2 = \left(\frac{1}{n} \sum_{i=1}^n x_i \right)^2$$

则其方差与标准离差可表示为：

$$\sigma_n^2 = \overline{x^2} - (\bar{x})^2 \quad \text{与} \quad \sigma_n = \sqrt{\overline{x^2} - (\bar{x})^2} \quad (7-7)$$

当数据个数较少时，统计学中可以证明上述计算式具有系统性误差。为了消除这种误差，在计算实践中当 n 较少时，通常采用无偏估计式：

$$\sigma_{n-1}^2 = \frac{1}{n-1} \left[\sum_{i=1}^n x_i^2 - n\bar{x}^2 \right] \quad (7-8)$$

$$\sigma_{n-1} = \sqrt{\frac{1}{n-1} \left[\sum_{i=1}^n x_i^2 - n\bar{x}^2 \right]} \quad (7-9)$$

同计算算术平均值的情况一样，当数组中有若干组相同数据时，其方差表达式可写为：

$$\sigma_n^2 = \sum_{j=1}^k (x_j - \bar{x})^2 w_j = \sum_{j=1}^k x_j^2 \bullet w_j - (\bar{x})^2 \quad (7-10)$$

或

$$\sigma_{n-1}^2 = \frac{1}{n-1} \sum_{j=1}^k (x_j - \bar{x})^2 \gamma_j = \frac{1}{n-1} \left[\sum_{j=1}^k x_j^2 \gamma_j - n(\bar{x})^2 \right] \quad (7-11)$$

(3) 数据的偏度及峰度

对于形为正态型等对称性分布来说，其均值、众数与中位数往往是同一个数值。对于非对称分布而言，往往采用偏度与峰度来描述其斜扭尖峰状况。

数据偏度的表达式为：

$$\{x_i\}_{\text{偏}} = \frac{\left(\frac{1}{n}\right) \sum_{i=1}^n (x_i - \bar{x})^3}{\sigma^3} \quad (7-12)$$

其简算式为:

$$\{x_j\}_{\text{偏}} = \frac{\text{均数} - \text{众数(或中位数)}}{\sigma} \quad (7-13)$$

数据峰度的表达式为:

$$\{x_i\}_{\text{峰}} = \frac{\frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^4}{\sigma^4} \quad (7-14)$$

例 7-1 中四组数据的极差、标准离差, 以及偏度峰度值如表 7-3 所示 (式中 σ 取 σ_{n-1})。

表 7-3 四组数据的分散性特征量

分 组	R	σ	σ_{n-1}	偏 度	偏度简算值	峰 度
A 组	4	1.247	1.291	0.53	1.03 (0.26)	1.98
B 组	4	1.155	1.225	0	0 (0)	1.78
C 组	4	1.199	1.282	0.40	0.59 (0.20)	1.78
D 组	4	1.199	1.282	-0.40	-0.59 (-0.20)	1.78

7.6.2 样本的频率分布

均值方差等虽然能反映一组数据的集中性和分散性, 但它们还不能完全反映一批数据的整个面貌。为了较完整地反映一批数据的统计规律, 往往需要对整批数据进行统计分组, 建立频率直方图。假定有 n 个观测数据, 分别以 $x_1, x_2, \dots, x_b, \dots, x_n$ 表示, 建立频率直方图的步骤是:

① 找出观测数据的极大值和极小值, 求出极差:

$$R = \max\{x_i\} - \min\{x_i\}$$

② 根据样本的大小进行分组。通常可分成 5~10 组。经验上也可采用如下简化公式来确定分组的数目 k , 即:

$$k = 1 + 3.31 \lg n$$

③ 根据组数 k 和极差 R 决定组距 C , 如果按等距分组, 则:

$$C \approx \frac{R}{K-1}$$

④ 确定各小组的端点值。端点值通常比原始数据的精度高一位, 使得原始数据不落在组区界限上。

- ⑤ 计算各组的频数 V_j 。
- ⑥ 计算各组的频率 $\frac{v_j}{n} = f_j$ 。
- ⑦ 以端点值为横坐标，以频率 v_j 或频率 f_j 为纵坐标画出直方图。

【例 7-2】 有 60 个数据，如表 7-4 所示。

表 7-4 60 个统计数据

91	77	55	58	105	32	64	64	64	46
98	47	67	30	84	53	78	37	97	25
60	80	73	47	40	69	50	77	13	79
43	82	61	37	73	38	49	48	50	66
76	57	44	60	87	29	112	87	43	21
57	59	32	64	75	47	71	69	55	72

乍一看，看不出这一组数据的性质。但仔细一看，便会发现小于 30 的数值很少，大于 100 的更少，而 40~70 最多，但更详细的情况就不清楚了。为了更好地了解这一组数据，就得采用直方图来进行分析。按照下列步骤绘制直方图：

- ① 这组数据的最大值为 112，最小值为 13，因而极差 $R=112-13=99$ 。
- ② 适当的选择分组数，分组太少则不足以说明数值的性质，分组过多则感到过于烦琐。按照经验公式 $k=1+3.3\lg 60=1+3.3\times 1.78=1+5.874=6.874$ 为好，因而选取 k 为 7。
- ③ 按等距离分组：

$$C=\frac{R}{k-1}=\frac{99}{7-1}=\frac{99}{6}=16.5$$

- ④ 确定初始端点值：

$$X_0=\min\{x_i\}-\frac{c}{2}=13-\frac{16.5}{2}=13-8.25=4.75$$

由此进行统计分组，数出频数，计算频率，如表 7-5 所示。

表 7-5 表 7-4 中数据的统计特征量

分组端点值	频数 v_j	频率 $f_j = \frac{v_j}{n}$	组中值
4.75~21.25	2	0.0333	13
21.25~37.75	7	0.1167	29.5
37.75~54.25	14	0.2333	46
54.25~70.75	17	0.2833	62.5
70.75~87.25	15	0.2500	79
87.25~103.75	3	0.0500	95.5
103.75~120.25	2	0.0333	112

由此可画出直方图如，图 7-12 所示。

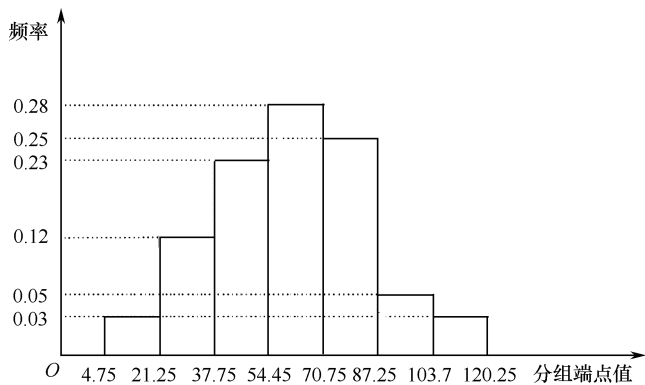


图 7-12 60 个数据的频率直方图

由上述直方图不难看出，这组数据具有中间大，两头小的分布特点，也就是说，这组数据的大多数点都密集在中心点附近，偏差中心的距离越远，其数据点的个数越少。

【例 7-3】 某种电子设备共 18 台，从开始使用到发生失效的时间数据如下：16，29，50，68，100，130，140，190，220，270，280，340，410，450，520，620，800，1100。

不难看出，这组数据的特点是初期失效较多，大部分数据都密集在前面。为了更好地了解这组数据的特点，需要将数据进行统计分组，绘制出频率直方图。按上述方法得：极差 $R=1100-16=1084$ ，选取 $k=6$ ，求出 $C=220$ ， $X_0=15.5$ 。

进行统计分组，得出频率分布表，如表 7-6 所示。

表 7-6 例 7-3 中所列数据的统计特征量

区间端点值	频数 v_j	频率 $f_j = \frac{v_j}{n}$	组中值
15.5~235.5	9	0.5	125.5
235.5~455.5	5	0.2778	345.5
455.5~675.5	2	0.1111	565.5
675.5~895.5	1	0.0556	785.5
895.5~1115.5	1	0.0556	1005.5

其频率直方图如图 7-13 所示。

比较上述两个频率直方图，不难看出，这两组数据是具有不同分布特点的。例 7-2 的数据大多数都密集在该组数据的中心，具有中间大、两头小的分布特性；例 7-3 的数据大多数都密集在初始阶段，具有前面较密，后面稀疏的分布特性。

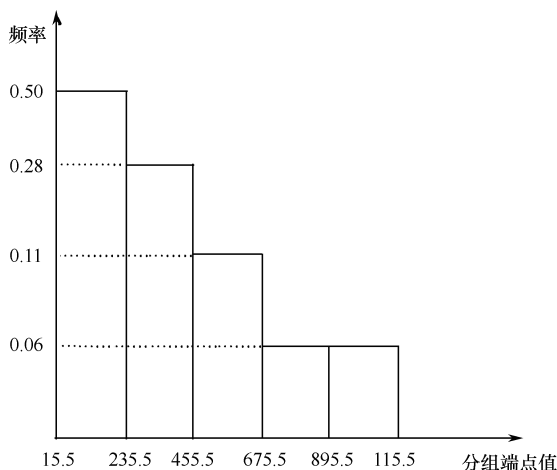


图 7-13 18 台样品数据的直方图

7.6.3 周期测量数据的统计处理

1. 参数性能的变化曲线

在寿命试验中，经常需要对一批样品的技术性能参数进行周期测量，以了解其随时间变化的参数漂移及稳定性情况。例如电容器要测试试验样品容量变化百分比 $\Delta C/C\%$ 、损耗角正切 $\text{tg}\delta$ 、绝缘电阻 R_{az} 等；晶体三极管要测试电流放大倍数 β 、漏电流 I_{ceo} 、饱和压降 V_{ces} 或它们的变化百分率等。

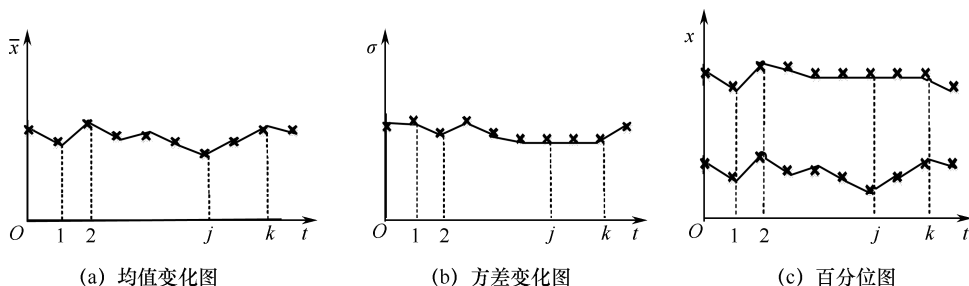
假定有 n 个样品投入试验，若用 x_i 来表示第 i 个样品的技术性能参数，则在每一个测试周期中都有 n 个性能参数值，因此每一个观测周期所得到的数据都是一组数据。显然，均值、标准离散等都可以作为一组数据的代表值。

除了均值方差等统计尺度以外，有时还采用百分位来表征这些数据。假定将 n 个测量值 $x_1, x_2, \dots, x_i, \dots, x_n$ 按大小次序进行排列，得到：

$$x_1 \leq x_2 \leq \dots \leq x_i \leq \dots \leq x_n$$

则将 $\frac{i}{n}$ 的百分比值 P 称为分位点。例如 $n=20, i=1$ ，则称 $\frac{i}{n} = \frac{1}{20} = \frac{5}{100}$ 为 5% 分位点。同样若 $n=20, i=10$ ，则称其为 50% 分位点。

如果对产品进行了 K 个周期的观测，假定第 j 个周期 ($j=0, 1, \dots, j, \dots, K$) 中 n 个数据的均值、标准离差、百分位分别为 $\bar{x}_j; \sigma_j; P_j (\%)$ ，则分别以 \bar{x}_j, σ_j, x_j 为纵坐标，以时间周期为横坐标，描出产品技术参数的均值、标准离差、百分位随时间的变化曲线。这 3 种曲线的示意图如图 7-14 所示。


 图 7-14 K 个周期观测值的统计量变化曲线

2. 周期测量数据失效时刻的划分

在周期测试中, 往往有这样的情况, 即样品失效发生在两个测试周期之间, 因而无法准确地知道每个样品的具体失效时刻。为了逐个计算产品的累积失效频率, 就需要对若干个周期失效产品的失效时刻进行分离。

假定第 $j-1$ 到第 j 个周期内, 样品的失效数为 v_j , 则它们的失效时刻可按下式进行计算:

$$t_{j,l} = t_{j-1} + \frac{t_j - t_{j-1}}{v_j + 1} \cdot l \quad l=1, 2, \dots, v_j \quad (7-15)$$

这样就可以将所有产品的失效时刻重新进行排队, 然后按大小次序计算产品的累积失效频率。若第 1 周期内失效 1 个, 第 2 周期内失效 3 个, 第 3 周期内失效 2 个, 则其累积失效频率如图 7-15 所示。

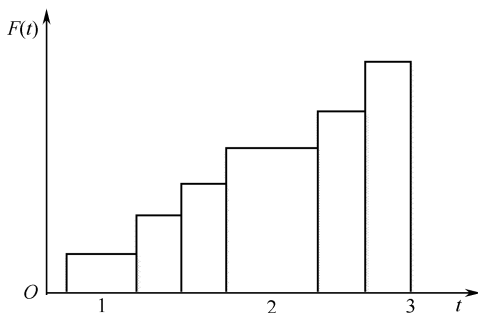


图 7-15 累积失效频率图

7.6.4 散布图

1. 散布图的绘制

为了比较两个变量之间的关系或比较试验前后产品特性值的相互关系, 往往需

要将试验数据绘制成散布图。散布图就是以 一个变量的值为横坐标，以另一个变量的值为纵坐标，在 x 、 y 坐标系中直接描点而绘制出来的图形。

【例 7-4】 某种型号的产品有 8 个样品，试验前的参数值为 x_i ($i=1, 2, \cdots, 8$)，试验后的参数值为 y_i ($i=1, 2, \cdots, 8$)，其数值如表 7-7 所示。

表 7-7 某型号产品 8 个样品的试验前后参数值

序 号	1	2	3	4	5	6	7	8
x_i	63	68	59	58	65	61	63	59
y_i	72	75	70	66	71	72	69	69

图 7-16 为根据表 7-7 的数据，以 x 为横坐标， y 为纵坐标，绘制出的散布图。

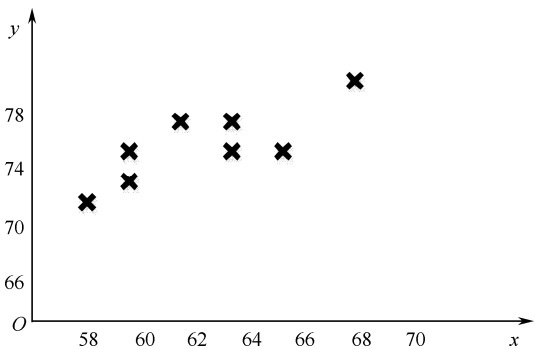


图 7-16 8 个样品数据的散布图

2. 相关与相关分析

在可靠性实践中，经常需要知道影响产品寿命的主要因素。例如想要掌握电动机转数、马力、使用环境、电刷等对电动机寿命的影响，就需要绘制散布图。在 n 个特性值中，如果其中某两个有着明显的因果关系，就称此两者是相关的。如果转数与寿命有较密切的关系，而马力大小对寿命几乎没有影响，就称电动机寿命与转数有关，而与马力无关。

表示因果关系大小的数值叫做相关系数。如果用 \bar{x} 、 σ_x 来表示变量 x_i 的均值和标准离差，用 \bar{y} 、 σ_y 来表示变量 y_i 的均值和标准离差，并定义协方差：

$$\sigma_{xy}^2 = \frac{1}{n-1} \sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y}) \tag{7-16}$$

则用各变数的标准离差的乘积去除协方差，所得到的值 r 称为相关系数：

$$\begin{aligned}
 r &= \frac{\sigma_{xy}^2}{\sigma_x \sigma_y} = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2 \cdot \sum_{i=1}^n (y_i - \bar{y})^2}} \\
 &= \frac{\sum_{i=1}^n x_i y_i - n \bar{x} \bar{y}}{\sqrt{\left(\sum_{i=1}^n x_i^2 - n \bar{x}^2 \right) \left(\sum_{i=1}^n y_i^2 - n \bar{y}^2 \right)}} \\
 &= \frac{\overline{xy} - \bar{x} \bar{y}}{\sqrt{\left(\overline{x^2} - (\bar{x})^2 \right) \left(\overline{y^2} - (\bar{y})^2 \right)}}
 \end{aligned} \tag{7-17}$$

式中:

$$\begin{aligned}
 \overline{xy} &= \frac{1}{n} \sum_{i=1}^n x_i y_i \\
 (\bar{x})^2 &= \left(\sum_{i=1}^n x_i / n \right)^2 \\
 \overline{x^2} &= \sum_{i=1}^n x_i^2 / n \\
 (\bar{y})^2 &= \left(\sum_{i=1}^n y_i / n \right)^2 \\
 \overline{y^2} &= \sum_{i=1}^n y_i^2 / n
 \end{aligned}$$

且当 n 较大时, 将 $n-1$ 与 n 同等待待。

例 7-4 中的 8 个数据有: $\bar{x} = 62$, $\sigma_x = 3.42$, $\bar{y} = 70.5$, $\sigma_y = 2.67$, 并按表 7-8 计算协方差。

表 7-8 例 7-4 中数据的协方差

序 号	1	2	3	4	5	6	7	8	Σ
① $x_i - \bar{x}$	1	6	-3	-4	3	-1	1	-3	
② $y_i - \bar{y}$	1.5	4.5	-0.5	-4.5	0.5	1.5	-1.5	-1.5	
①×②	1.5	27	1.5	18	1.5	1.5	1.5	4.5	51

因此根据相关系数公式可以得到:

$$r = \frac{\sigma_{xy}^2}{\sigma_x \sigma_y} = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{(n-1) \sigma_x \sigma_y}$$

$$= \frac{51}{7 \times 3.42 \times 2.67} = \frac{51}{7 \times 9.1314}$$

$$= \frac{51}{63.92} = 0.8$$

也就是说，该例题中数据的相关系数为 0.8。

相关系数的大小表示两组数据的相关程度。若 $|r|=1$ 就称为完全线性相关， $|r|=0$ 就称为全无线性相关； $|r|$ 越接近于 1，线性相关越大； $r=+1$ 时称为正相关， $r=-1$ 时称为负相关。上例的 $r=0.8$ ，可见其相关程度比较好。不同的散布图有不同的相关系数，不同的相关系数也有不同形式的散布图。几种典型的散布图如图 7-17 所示。

为了有效地判断变量之间是否确实相关，往往还需要对相关系数进行恰当的检验。一般可采用专门编制的检验表，根据数据的个数 n 及显著性水平 α ，对相关系数进行显著性检验。上例的 $n=8$ ，取 $\alpha=0.05$ ，查表得 0.707，由 $r=0.8 > 0.707$ ，因此有 95% 的置信度认为例题中的相关系数是有效的。

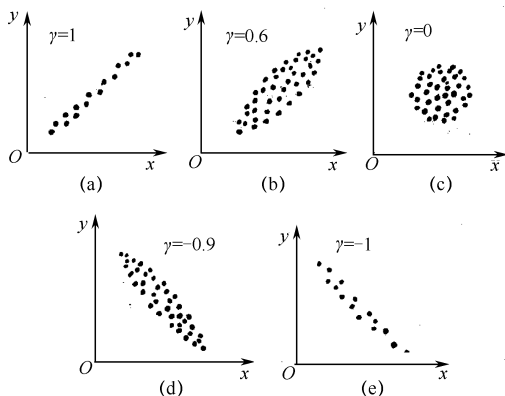


图 7-17 几种不同情况的散布图

相关分析是用来检验两个参数之间的独立性的。例如继电器的接点电阻值与寿命的关系、电阻噪声值与寿命的关系，经相关分析检验后，若其相关系数具有极大的显著性，就可以作为寿命特性来使用。

7.6.5 回归分析

在两个相关的特性值中，当一方变化，另一方也随之变化时，需要找出相应的方程式，这种工作叫做回归。该方程式就叫回归方程式。从观测数据中求此方程式的过程，叫做回归分析。回归分析中较常用的方法是最小二乘法。

设 \hat{y}_i 为与 x_i 所对应的观测值, y_i 为其理论值。如果变量间存在着线性关系, 则可用直线 $y=a+bx$ 来拟合它们之间的变化关系。最小二乘法就是选取方程中的 a 、 b 使得误差平方和为最小的拟合方法。由于误差平方和为

$$\varepsilon = \sum_{i=1}^n [\hat{y}_i - (a + bx_i)]^2 \quad (7-18)$$

将它们分别对 a 、 b 求偏导数, 并令其为 0, 则有:

$$\begin{aligned} \frac{\partial \varepsilon}{\partial a} &= \sum_{i=1}^n 2[y_i - (a + b\hat{x}_i)][-1] = 0 \\ \frac{\partial \varepsilon}{\partial a} &= \sum_{i=1}^n 2[\hat{y}_i - (a + b\hat{x}_i)][-x_i] = 0 \end{aligned}$$

由此可得:

$$a = \frac{\sum_{i=1}^n y_i}{n} - \frac{\sum_{i=1}^n x_i}{n} b = \bar{y} - b\bar{x} \quad (7-19)$$

$$b = \frac{\sum_{i=1}^n x_i y_i - \bar{y} \sum_{i=1}^n x_i}{\sum_{i=1}^n x_i^2 - \bar{x} \sum_{i=1}^n x_i} = \frac{\overline{xy} - \bar{y}\bar{x}}{x^2 - (\bar{x})^2} \quad (7-20)$$

另一方面, 由于:

$$\frac{\sigma_{xy}^2}{\sigma_x^2} = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sum_{i=1}^n (x_i - \bar{x})^2} = \frac{\sum_{i=1}^n x_i y_i - n\bar{x}\bar{y}}{\sum_{i=1}^n x_i^2 - n(\bar{x})^2} = \frac{\overline{xy} - \bar{x}\bar{y}}{x^2 - (\bar{x})^2}$$

得:

$$b = \frac{\sigma_{xy}^2}{\sigma_x^2} \quad a = \bar{y} - b\bar{x} \quad (7-21)$$

对例 7-4 中的 8 对数据列表进行计算, 如表 7-9 所示。

表 7-9 例 7-4 中数据的回归分析计算结果

	x_i	y_i	$x_{i0} = x_i - \bar{x}$	$y_{i0} = y_i - \bar{y}$	$x_{i0} y_{i0}$	x_{i0}^2	y_{i0}^2
	63	72	1	1.5	1.5	1	2.25
	68	75	6	4.5	27.0	36	20.25
	59	70	-3	-0.5	1.5	9	0.25
	58	66	-4	-4.5	18.0	16	20.25
	65	71	3	0.5	1.5	9	0.25
	61	72	-1	1.5	-1.5	1	2.25
	63	69	1	-1.5	-1.5	1	2.25
	59	69	-3	-1.5	4.5	9	2.25
Σ	496(Σ)	564(Σ)			51(Σ)	82(Σ)	50(Σ)



由上表可以得到:

$$b = \frac{\sum_{i=0}^n x_{i0} y_{i0}}{\sum_{i=0}^n x_{i0}^2} = \frac{51}{82} = 0.62$$

$$a = \frac{\sum_{i=0}^n y_i}{n} - b \frac{\sum_{i=0}^n x_i}{n} = \frac{564}{8} - 0.62 \frac{496}{8}$$

$$= 70.5 - 0.62 \times 62 = 32$$

因而该例中散布图的回归直线方程式为:

$$y = 0.62x + 32$$

7.6.6 方差分析

为了比较 r 组数据之间是否具有显著性差异, 可以借用数理统计中的方差分析方法。方差分析方法有单因素方差分析与多因素方差分析等方法。为了简便起见, 本节只介绍单因素的方差分析方法。

设有 r 组相互独立的数据, 每组中又有 n_i 个观测值。将其表达为:

$$\{x_{ij}\} \quad (i=1, 2, \dots, r) \quad (j=1, 2, \dots, n_i) \quad (7-22)$$

令其总平均值为

$$\bar{x} = \frac{1}{n} \sum_{i=1}^r \sum_{j=1}^{n_i} x_{ij} \quad (n = \sum_{i=1}^r n_i) \quad (7-23)$$

则可以构造其统计量:

$$Q = \sum_{i=1}^r \sum_{j=1}^{n_i} (x_{ij} - \bar{x})^2$$

这个统计量是用来描述观测信息与总平均值 \bar{x} 的离散程度的。

实际上, 上述统计量可以分解为两部分, 即:

$$Q = Q_1 + Q_2$$

式中:

$$Q_1 = \sum_{i=1}^r \sum_{j=1}^{n_i} (x_{ij} - \bar{x}_i)^2$$

$$Q_2 = \sum_{i=1}^r n_i (\bar{x}_i - \bar{x})^2$$

$$\bar{x}_i = \frac{1}{n_i} \sum_{j=1}^{n_i} x_{ij}$$

不难看出, Q_1 反映了各子样观测值与 \bar{x}_i 之间的离散程度; Q_2 反映了 \bar{x}_i 的均值

与总平均值 \bar{x} 之间的离散程度。

在统计学中，构造了统计量：

$$S_1^2 = \frac{1}{n-r} Q_1$$

$$S_2^2 = \frac{1}{r-1} Q_2$$

并且已证明： $F = \frac{S_2^2}{S_1^2}$ 是服从参数为 $r-1, n-r$ 的 F 分布的。对于给定的 α 可在 F 颁布表中查得 F_α 。

由观察计算所得到的 F ，若大于查表值 F_α ，就说明 S_2^2 显著地大于 S_1^2 ，即组与组之间的离差显著地大于组内部的离差，因而它们之间有显著性差异。由实测数据中算出的 F 值，若小于 F_α ，则说明它们之间无显著性差异。

【例 7-5】 对 7 种不同型号的电视机进行可靠性试验，分别得到 7 组数据，如表 7-10 所示。

表 7-10 7 种不同型号的电视机可靠性试验数据（单位：10² 小时）

	A_1	A_2	A_3	A_4	A_5	A_6	A_7	\bar{x}
1	40	40	40	2.4	40	40	40	
2	24	40	40	40	40	40	40	
3	40	40	40	24	40	24		
4	40	40	24	40	24			
5	24	40	40	40	24			
6	24		40	40	40			
7			40	24				
\bar{x}_i	32	40	37.71	33.14	34.67	34.67	40	35.56
n_i	6	5	7	7	6	3	2	
ε_i	384	0	219.43	438.86	341.33	170.67	0	

表中：

$$\bar{x} = \frac{1}{n} \sum_{i=1}^r \sum_{j=1}^{n_i} x_{ij}$$

$$\bar{x}_i = \frac{1}{n_i} \sum_{j=1}^{n_i} x_{ij}$$

$$\varepsilon_i = \sum_{j=1}^{n_i} (x_{ij} - \bar{x}_i)^2$$



由上表计算得:

$$Q_1 = \sum_{i=1}^r \varepsilon_i = 1554.29$$

$$S_1^2 = \frac{Q_1}{n-r} = 1554.29 / 29 = 53.60$$

$$\theta_2 = 294.52$$

$$S_2^2 = \frac{\theta_2}{r-1} = \frac{294.52}{6} = 49.09$$

故有:

$$F = S_2^2 / S_1^2 = 49.09 / 53.60 = 0.9158$$

查表得:

$$F_{\alpha} = F_{0.1}(6, 29) = 1.99$$

由于 $F < F_{0.1}(6, 29)$, 说明 7 种电视机的可靠性水平之间没有显著性差异。

7.7 可靠性数据分析的数学方法

7.7.1 分布类型检验

1. 概述

试验观测数据是否服从某种理论分布, 需要进行拟合检验。由图估法不难看出, 产品分布的理论值在概率纸上应该是一条理想的直线, 而产品样本的实测值却往往在直线附近摆动, 也就是说, 子样的实测值是分布在母体理论值的周围的。于是理论分布与实测分布之间的偏差又形成了一种新的分布。如果能够构造一个反映理论值与实测值偏差值的统计量, 并且能够确定这种统计量的分布类型, 那么就可以根据这个统计量分布类型的允许范围, 对实测值与理论值之间是否相符合给出判断。

假定构造的统计量为 μ , 并且已知 μ 是服从 μ_{α} 分布的, 其中 α 为 μ 分布的 α 分位点, 并且设 α 是一个较小的数, 例如 $\alpha=0.05, 0.01, 0.10$ 等等。如果有下列式子成立:

$$P(\mu \geq \mu_{\alpha}) = \alpha$$

就称事件 “ $\mu \geq \mu_{\alpha}$ ” 为小概率事件。

由概率论可知, 小概率事件在一次试验中几乎是不可能发生的, 也就是说, 一般来说事件 “ $\mu \geq \mu_{\alpha}$ ” 是不会发生的, 如果发生了, 表明这一事件不可信, 或者

说这一事件发生的可能性只有 α ，有 $1-\alpha$ 的把握相信它不会发生。

如果事件 “ $\mu \geq \mu_\alpha$ ” 不发生，表明这一事件是可信的，或者说这一事件不出现的可能性有 $1-\alpha$ ，因此有 $1-\alpha$ 的把握相信事件 “ $\mu \geq \mu_\alpha$ ” 不会发生，或者说 $1-\alpha$ 的把握相信会出现事件 “ $\mu < \mu_\alpha$ ”。

为此，我们将 α 称为显著性水平，将 $1-\alpha$ 称为置信度。

综上所述，对产品寿命分布进行拟合检验的基本思想是：首先根据以往的经验，根据样本直方图的几何形状、实测数据在各种概率纸上的拟合程度，对母体的分布类型做出假设；然后构造一个能够反映理论值与实测值偏差的统计量，在已知统计量的精确分布或渐近分布的前提下，根据一定的置信度来选取判别标准，最后再将统计量的计算值与判别标准进行比较，做出接受原假设或拒绝原假设的判决。

分布检验的基本步骤如图 7-18 所示。

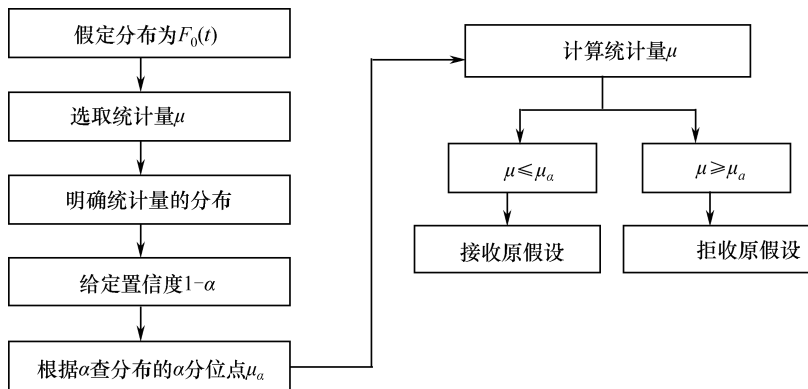


图 7-18 进行分布拟合检验的基本步骤

确定寿命分布类型的拟合检验方法比较多。在具体应用过程中，只要选取合理的统计量，并查找统计量所趋分布的 α 分位点就可以了。关于统计量的构造方法及其统计量分布的表格制订，请参阅有关数理统计方面的资料。下面只叙述 χ^2 检验、K-S 检验以及对各种分布类型进行检验的步骤和应用。

2. 皮尔逊检验

皮尔逊检验又称 χ^2 检验，一般只用于大样本，且一般将数据分组。 χ^2 检验的使用范围很广，能够用于连续分布和离散分布，也可用于分布参数是由极大似然估计得来的情况。可用于母体分布的参数已知，也可用于参数未知；可以用于完全样本，也可用于截尾样本和分组数据。

在 χ^2 检验中，把观察频数与理论频数之差的平方除以理论频数，然后将所得的

商相加，就得到了 χ^2 统计量，即：

$$\chi^2 = \sum_{i=1}^k \frac{(v_i - np_i)^2}{np_i} \tag{7-24}$$

式中： k 为将数据进行统计分组的组数； v_i 为落入每个子区间内的观察失效频数， p_i 为落入每个子区间内的理论概率； n 为观察样本的总数，因而 np_i 就为应该落入子区间的理论频数。

可以证明，统计量 χ^2 是服从以 $k-1$ 为自由度的 χ^2 分布的，因此，对观测数据进行 χ^2 检验的步骤是：

- ① 假定产品服从寿命分布 $F_0(t)$ 。
- ② 根据 n 个观察数据的范围，将失效时间分成 k 个子区间 $[t_i, t_{i+1}] (i = 1, 2, 3, \cdots, k)$ ，使每个子区间内的失效观察频数 $v_i \geq 5$ ；
- ③ 统计观察数据落入每个子区间的经验频数 v_i 。
- ④ 按公式 $p_i = F_0(t_{i+1}) - F_0(t_i) = p(t_i \leq T < t_{i+1})$ 计算应落入子区间内的理论概率 p_i ，并计算应落入该区间的理论频数 np_i 。
- ⑤ 由公式 $\chi^2 = \sum_{i=1}^k \frac{(v_i - np_i)^2}{np_i}$ 计算统计量。
- ⑥ 以 $(k-1)$ 为自由度，并根据给定的置信度 $1-\alpha$ 查 χ^2 分布的下侧分位数表得 $\chi^2_{1-\alpha}(k-1)$ 。
- ⑦ 将统计量的观察值 χ^2 与判别标准 $\chi^2_{1-\alpha}(k-1)$ 进行比较：
 - 若 $\chi^2 < \chi^2_{1-\alpha}(k-1)$ ，则认为产品属于 $F_0(t)$ 分布（置信度 $1-\alpha$ ）。
 - 若 $\chi^2 \geq \chi^2_{1-\alpha}(k-1)$ ，则认为产品不服从 $F_0(t)$ 分布，需要另做假设再进行检验。

上述检验步骤适用于已知 $F(t)$ 的分布参数，若 $F(t)$ 的 1 个分布参数需要以参数估计方法来确定时，则 χ^2 分布的下侧分位数的自由度应改为 $k-1-l$ ，也就是说，检验标准应由 $\chi^2_{1-\alpha}(k-1)$ 改为 $\chi^2_{1-\alpha}(k-1-l)$ 。

关于统计量的计算过程如表 7-11 所示。

表 7-11 皮尔逊检验统计量的计算过程

区间序号 i	区间 $[t_i, t_{i+1}]$	观察频数 v_i	理论频率 p_i	理论频数	$(v_i - np_i)^2 / np_i$
1	$t_1 - t_2$	v_1	p_1	np_1	$(v_1 - np_1)^2 / np_1$
2	$t_2 - t_3$	v_2	p_2	np_2	$(v_2 - np_2)^2 / np_2$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
i	$t_i \sim t_{i+1}$	v_i	p_i	np_i	$(v_i - np_i)^2 / np_i$

(续表)

区间序号 i	区间 $[t_i, t_{i+1}]$	观察频数 ν_i	理论频率 p_i	理论频数	$(\nu_i - np_i)^2 / np_i$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
k	$t_k \sim t_{k+1}$	ν_k	p_k	np_k	$(\nu_k - np_k)^2 / np_k$
Σ					$\sum_{i=1}^k \frac{(\nu_i - np_i)^2}{np_i}$

【例 7-6】某 60 个产品进行试验后，得到的统计分组结果如表 7-12 所示（左半部）。假设它服从正态分布 $N(61.22, 21.45)$ ，现取 $\alpha = 0.05$ ，对它进行 χ^2 检验。

由于假定它服从 $N(61.22, 21.45)$ ，所以有：

$$F_0(t) = \Phi\left(\frac{t - 61.22}{21.45}\right)$$

按照 $P_i = \Phi\left(\frac{t_{i+1} - \mu}{\sigma}\right) - \Phi\left(\frac{t_i - \mu}{\sigma}\right)$ 计算各区间的理论概率后，列表计算如表 7-12 所示。

表 7-12 某产品试验数据和 χ^2 检验结果

序号 i	$t_i \sim t_{i+1}$	ν_i	p_i	np_i	$(\nu_i - np_i)^2 / np_i$
1	3.75~36.75	7	0.1234	7.4	0.0216
2	36.75~53.25	16	0.2287	13.722	0.378
3	53.25~69.75	17	0.2998	17.9898	0.0544
4	69.75~86.25	12	0.2236	13.416	0.149
5	86.25~119.25	8	0.1176	7.056	0.129
Σ					$\chi^2 = 0.729$

查 χ^2 分位表得：

$$\chi_{1-\alpha}^2(k-1) = \chi_{0.95}^2(4) = 9.488$$

由于 $\chi^2 = 0.729 < 9.488 = \chi_{1-\alpha}^2(k-1)$ ，所以接受原假设。

3. K-S 检验

K-S 检验的全称是柯尔莫哥洛夫-斯米尔诺夫检验，简称柯氏检验。设 $F_0(t)$ 为随机变量 T 的理论分布， $F_n(t)$ 为实测数据的经验分布，则将下式：

$$D_n = \sup_{-\infty < t < \infty} |F_n(t) - F_0(t)| \quad (7-25)$$

作为衡量理论分布与经验分布之间的偏差的变量，显然 D_n 是一个统计量。 D_n 表示了 $F_n(t)$ 与 $F_0(t)$ 之差的最大绝对值。如果经验分布和理论分布相当接近， D_n 不应很大。如果给定一个最大允许范围 $D_{n,\alpha}$ ，则当 $D_n > D_{n,\alpha}$ 时，就说明子样的经验

分布 $F_n(t)$ 不接近于预先假定的理论分布 $F_0(t)$ ， $D_{n,\alpha}$ 由 $P(D_n > D_{n,\alpha}) = \alpha$ 确定。在 $F_0(t)$ 为连续分布的条件下，对于不同的 α 和 $n=1\sim 30$ ，统计学中已经给出了 $D_{n,\alpha}$ 的数表。

因此，对产品寿命分布进行 K-S 检验的步骤是：

- ① 假定产品服从寿命分布 $F_0(t)$ 。
- ② 将产品失效时间按大小顺序进行排列： $t_1 \leq t_2 \leq \dots \leq t_i \leq \dots \leq t_n$ 。
- ③ 按假设分布的理论公式计算 $F_0(t)$ 的理论值，得到 $F_0(t_i)$ 。
- ④ 按公式 $F_n(t_i) = \frac{i}{n}$ 计算子样累积失效频率的值。
- ⑤ 按公式 $|F_n(t_i) - F(t_i)|$ 计算理论值与实测值的绝对差，并找到最大值，得到 D_n 。
- ⑥ 由给定的置信度 $1-\alpha$ ，查 K-S 检验临界值 L_n 表，得 $D_{n,\alpha}$ 。
- ⑦ 将 D_n 与 $D_{n,\alpha}$ 进行比较。
 - 若 $D_n < D_{n,\alpha}$ ，则认为产品属于 $F_0(t)$ 分布。
 - 若 $D_n \geq D_{n,\alpha}$ ，则认为产品不服从 $F_0(t)$ 分布，需要另做假设再进行检验。

【例 7-7】 从一批产品中随机抽取 10 只样品做寿命试验，得到如下 10 个数据（以小时为单位）：**1.0、2.0、4.5、5.5、6.0、8.0、12、19、25、70**，希望利用这 10 个数据，判断其分布是否符合平均寿命为 10 小时的指数分布。

解：① 按表 7-13 计算 D_n 。

表 7-13 随机抽取样品的试验数据和统计量值

序 号	t_i	$F_n(t_i) = \frac{i}{n}$	$F_n(t_i)$	$ F_n(t_i) - F(t_i) $
1	1.0	0.1	0.0952	0.0048
2	2.0	0.2	0.1813	0.0181
3	4.4	0.3	0.3624	0.0624
4	5.5	0.4	0.4231	0.0231
5	6.0	0.5	0.4512	0.0488
6	8.0	0.6	0.5507	0.0493
7	12	0.7	0.6988	0.0012
8	19	0.8	0.8504	0.0504
9	25	0.9	0.9179	0.0179
10	70	1.0	0.9991	0.0009

表中：

$$F_0(t_i) = 1 - e^{-\frac{t_i}{10}}$$

不难看出 $|F_n(t_i) - F_0(t_0)|$ 的最大值为 $D_n = 0.0624$ 。

② 计算临界值 $D_{n,\alpha}$ ：设定 $\alpha = 0.20$ ，又知 $n = 10$ ，由 K-S 检验表查得 $D_{10,0.2} = 0.3226$ 。

③ 比较 D_n 和 $D_{n,\alpha}$ ：因为 $0.0624 < 0.3226$ ，即 $D_n < D_{n,\alpha}$ ，所以，可以有 80% 的把握相信它是服从以 10 小时为平均寿命的指数分布的。

上述检验方法适用于完全子样的情况，当 n 很大时，还可以找到 D_n 的极限分布表，作为判别标准。

对于连续分布 $F(t)$ ，统计学中可以证明有：

$$\lim_{n \rightarrow \infty} \left[D_n < \frac{\lambda}{\sqrt{n}} \right] = \sum_{k=-\infty}^{\infty} (-1)^k e^{-2k^2} \lambda^2 = \theta(\lambda) \quad (7-26)$$

对于给定的 α ，令 $\theta(\lambda) = 1 - \alpha$ ，则由 D_n 的极限分布表上可以找到对应的 λ 值，因而也就确定了进行检验的比较标准。

除上述完全子样的情况外，由于寿命试验、截尾试验，以及定时截尾与定数截尾等各种情况，因此，把它们的检验公式及步骤列于表 7-14 中。

表 7-14 χ^2 与 K-S 检验公式表

检验类型		统计量	否定域	备 注
χ^2 检验		$\chi^2 \geq \sum_{i=1}^k \frac{(v_i - np_i)^2}{np_i}$	$\chi^2 \geq \chi_{1-\alpha}^2(k-1)$	k 为分组数； v 为落入子区间的经验频数； p_i 为落入子区间的理论概率， $p_i = F(t_{i+1}) - F(t_i)$ ； $\chi_{1-\alpha}^2(k-1)$ 是下侧分位数的 χ^2 表
柯氏 (K-S) 检验	完全子样	$D_n = \text{Sup} F_n(t) - F(t) $ $-\infty < t < \infty$	$D_n > D_{n,\alpha}$	Sup 表示 $F_n(t)$ 之差的绝对值的最大值， $D_{n,\alpha}$ 可根据 n 和 α 查柯氏检验 $D_{n,\alpha}$ 临界值表
	完全子样 (n 很大时)	$D_n = \text{Sup} F_n(t) - F(t) $ $-\infty < t < \infty$	$D_n > \frac{\lambda}{\sqrt{n}}$	λ 可根据 n 及 $1-\alpha$ 查 D_n 的极限分布表
	定数截尾	$T_r = \text{Sup} F_n(t) - F(t) $ $t \leq t_r$	$T_r > T_{n,\alpha}$	$T_{n,\alpha} = \frac{K}{n}$ K 可根据 n 、 r 及 $1-\alpha$ 查定数截尾临界值表
	定时截尾	$T_0 = \text{Sup} F_n(t) - F(t) $ $t \leq t_u$	$T_0 > T_{n,\alpha}$	t_u 为截尾时间，令 $R_0 = nF(t_u)T_{u,\alpha} = \frac{K}{n}$ ， K 可根据 $R_{c,n,1-\alpha}$ 查定时截尾临界值表
	截尾试验 ($n > 30$)	$D_{n,T} = \text{Sup} F_n(t) - F(t) $ $0 \leq t < T$	$\sqrt{n}D_{n,T} > D_{r,\alpha}$	T 为截尾时间， $D_{r,\alpha}$ 可根据 $F(T)$ 及 $G_T(\alpha) = 1 - \alpha$ 查截尾试验 $D_{n,T}$ 的极限分布表

4. 指数分布的假设检验

在可靠性工程实践中，经常使用指数分布模型来描述产品的失效规律。产品的失效是否符合指数模型或具有恒定失效率规律，往往需要通过实际数据来进行验证。GB/T 5080.6 给出了恒定失效率假设的有效性检验方法，可采用 χ^2 拟合优度检验法，失效总数为 r 个的试验样本，采用统计量：

$$\chi^2 = 2 \sum_{k=1}^d \ln\left(\frac{T^*}{T_k}\right) \tag{7-27}$$

式中： T_k 表示至第 k 次失效时的累积试验时间； T^* 表示总累积试验时间； d 是与失效数有关的参数，当有效性检验实施时刻与第 k 次失效出现的时刻相同时， $d=r-1$ ；否则， $d=r$ 。对于 $r>40$ 的情形，GB/T 5080.6 还给出了另一种检验方法，有兴趣的读者可查阅。

可以证明，对于显著性水平 $\alpha=0.10$ ，接受恒定失效率的肯定域为 $\left[\chi^2_{0.05}(2d), \chi^2_{0.95}(2d)\right]$ 。

如果 $\chi^2 < \chi^2_{0.05}(2d)$ ，则拒绝恒定失效率的假设，其失效率很可能是递增的；如果 $\chi^2 > \chi^2_{0.95}(2d)$ ，则也拒绝恒定失效率的假设，其失效率很可能是递减的。

【例 7-8】 对 4 部电台进行了累积 2114 小时的可靠性试验，试验中共有 8 次故障，其失效时间为：11.5、80、148、294、318、376、428、464。现对其进行恒定失效率假设的有效性检验。由于检验时间不是在出现某个失效时进行的，所以取 $d=r=8$ 。其检验的计算结果如表 7-15 所示。

表 7-15 对 4 部电台可靠性试验数据的检验计算结果

失效次数 i	1	2	3	4	5	6	7	8	Σ
失效时间（小时） t_i	11.5	80	148	294	318	376	428	464	
$T_k = 4 \times t_i$	46	320	592	1176	1272	1504	1712	1856	
T^*/T_k	45.96	6.61	3.57	1.80	1.66	1.41	1.23	1.14	
$\ln T^*/T_k$	3.83	1.89	1.27	0.59	0.51	0.34	0.21	0.13	8.76

$$\because \chi^2 = 2 \sum_{k=1}^8 \ln(T^*/T_k) = 17.53$$

查表得：

$$\chi^2_{0.05}(16) = 7.96, \quad \chi^2_{0.95}(16) = 26.3$$

由于 $\chi_{0.05}(16) < \chi^2 < \chi_{0.95}(16)$ ，所以接受该产品是恒定失效率的假设。

5. 正态型的假设检验

对于正态型分布，利里福斯给出了用 $\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i$ 代替未知均值，用 $S^2 = \frac{1}{n-1} \sum_{i=1}^n (x_i - \bar{x})^2$ 代替未知方差的模拟 K-S 检验。该检验的统计量为

$$\hat{D}_n = \max_{1 \leq i \leq n} (\hat{\delta}_i) \tag{7-28}$$

其中：

$$\hat{\delta}_i = \max \left[\Phi \left(\frac{x - \bar{x}}{s} \right) - \frac{i-1}{n}, \frac{i}{n} - \Phi \left(\frac{x - \bar{x}}{s} \right) \right]$$

其肯定域为

$$\hat{D}_n < D_n$$

\hat{D}_n 的表格如表 7-16 所示。

表 7-16 正态模型 K-S 检验表

样 本 数 <i>n</i>	置 信 度				
	0.20	0.15	0.10	0.05	0.01
4	0.300	0.319	0.352	0.381	0.417
5	0.285	0.299	0.315	0.337	0.405
6	0.265	0.277	0.294	0.319	0.364
7	0.247	0.258	0.276	0.300	0.348
8	0.233	0.244	0.261	0.285	0.331
9	0.223	0.233	0.249	0.271	0.311
10	0.215	0.224	0.239	0.258	0.294
11	0.206	0.217	0.230	0.249	0.284
12	0.199	0.212	0.223	0.242	0.275
13	0.190	0.202	0.214	0.234	0.268
14	0.183	0.194	0.207	0.227	0.261
15	0.177	0.187	0.201	0.220	0.257
16	0.173	0.182	0.195	0.213	0.250
17	0.169	0.177	0.189	0.206	0.245
18	0.166	0.173	0.184	0.200	0.239
19	0.163	0.169	0.179	0.195	0.235
20	0.160	0.166	0.174	0.190	0.231
25	0.142	0.147	0.158	0.173	0.200
30	0.131	0.136	0.144	0.161	0.186
>30	$\frac{0.736}{\sqrt{n}}$	$\frac{0.768}{\sqrt{n}}$	$\frac{0.805}{\sqrt{n}}$	$\frac{0.886}{\sqrt{n}}$	$\hat{\eta} = (\overline{t^m})^{1/m}$

【例 7-9】 现有 8 个寿命试验数据，其自然对数为：0.26、0.53、0.88、1.22、1.76、2.44、3.41、4.90。现要检验它们是否来自对数正态母体。

容易得到 $\bar{x}=1.925$ ， $S^2=2.522$ ，其统计量的计算过程如表 7-17 所示。

由表 7-16 可以看出 $\hat{D}_n = \max_{1 \leq i \leq n} (\delta_i) = 0.170$ ，查表 7-16 得 $D_n(\alpha) = D_8(0.20) = 0.233$ ，由于 $\hat{D}_n < D_n(\alpha)$ ，故接受该样本来源于对数正态母体的假设。

表 7-17 正态型假设检验的计算过程及结果

$x_i = \ln t_i$	0.26	0.53	0.88	1.22	1.76	2.44	3.41	4.90
$y_i = \frac{x_i - 1.925}{1.588}$	-1.05	-0.88	-0.66	-0.44	-0.10	0.32	0.94	1.87
$\Phi(y_i)$	0.147	0.189	0.255	0.330	0.460	0.626	0.826	0.969
$\frac{i-1}{n}$	0	0.125	0.25	0.375	0.5	0.625	0.75	0.875
i/n	0.125	0.25	0.375	0.5	0.625	0.75	0.875	1
$\Phi(y_i) - \frac{i-1}{n}$	0.147	0.064	0.005	-0.045	-0.04	0.001	0.076	0.094
$\frac{i}{n} - \Phi(y_i)$	-0.022	0.061	0.120	0.170	0.165	0.124	0.049	0.031

6. 威布尔或极值分布的检验

人们对威布尔分布的拟合检验进行了很多的研究，分别提出了 W 检验法、S 检验法及 P 检验法。现以 S 检验为例，对其检验法进行简单说明。S 检验的统计量是：

$$S_i = \sum_{(r/2)+1}^{r-1} l_i / \sum_1^{r-1} l_i \quad (7-29)$$

$$l_i = \frac{x_{i+1} - x_i}{E(Z_{i+1}) - E(Z_i)}$$

$$Z_i = \frac{x_i - \mu}{\sigma}$$

式中， μ 为位置参数； σ 为尺度参数； $E(Z_i)$ 为随机变量 Z_i 的期望值。对于 (n, r) 的样本，R.Mann 等人已给出了 S 分布的百分位点及 $E(Z_{i+1}) - E(Z_i)$ 的值。检验时，将实际计算值 S 与其临界值 $S_{n,r}(\alpha)$ 进行比较，就可给出接受或拒绝原假设的结论。

【例 7-10】 现有 $n=16$ ， $r=9$ 的试验数据为：15.5、16.5、19.5、20.5、23.1、

23.5、26.5、33.8、33.9。现检验它们是否来自于二参数的威布尔分布。其检验过程如表 7-18 所示。

表 7-18 威布尔分布检验过程及结果

i	t_i	$x_i = \ln t_i$	$x_{i+1} - x_i$	$E(Z_{i+1}) - E(Z_i)$	l_i
1	15.5	2.74	0.06	1.033	0.06
2	16.5	2.80	0.17	0.535	0.32
3	19.5	2.97	0.05	0.370	0.14
4	20.5	3.02	0.12	0.289	0.42
5	23.1	3.14	0.02	0.242	0.08
6	23.5	3.16	0.12	0.212	0.57
7	26.5	3.28	0.24	0.192	1.25
8	33.8	3.52	0	0.179	0
9	33.9	3.52			

表中 $E(Z_{i+1}) - E(Z_i)$ 的值是查 S 分布百分点和期望值差而得到的。根据上式结果, 可以得到:

$$S = \sum_{i=5}^8 l_i / \sum_{i=1}^8 l_i = 1.9 / 2.84 = 0.67$$

取 $\alpha = 0.20$, 查表有 $S_{16,9} = 0.65$ 。由于 S 大于临界值, 故拒绝接受它们来自二参数威布尔母体的假设。

7. 不同分布类型的鉴别

在试验数据处理中, 有时希望在两个指定的分布模型中选择其中一个模型。为了区别两个具有未知参数的分布, 可以采用似然比检验法。这些检验法的统计量如表 7-19 所示。表中 \bar{x} 为正态分布均值的极大似然估计量; $\hat{\sigma}_2$ 为对数正态分布对数方差的极大似然估计量; $f_w(x_i; \hat{m}; \hat{\eta})$ 为威布尔分布的密度函数; \hat{m} 为形状参数的极大似然估计量; $\hat{\eta}$ 为真尺度参数的极大似然估计量; D_{NE}^* 见表 7-20; D_{EN}^* 见表 7-21; D_{LNW}^* 见表 7-22; D_{WLN}^* 见表 7-23。

表 7-19 似然比检验公式表

分布	原假设	备择	统计量	肯定域
指数与正态	$\ln L(\mu, \sigma) = r(\ln 1 - \ln \sqrt{2\pi} - \ln \sigma) +$ $\ln l - \sum_{i=1}^r \ln t_i - \frac{1}{2\sigma^2} \sum_{i=1}^r (\ln t_i - \varpi)^2 +$ $(n-r) \ln \Phi(-z)$	$E(\alpha, \lambda)$	$D_{NE} = \frac{\sqrt{n \sum_{i=1}^n (x_i - \bar{x})^2}}{\sum_{i=1}^n (x_i - \min x_i)}$	$D_{NE} < D_{NE}^*$

(续表)

分布	原假设	备择	统计量	肯定域
指数与正态	$E(\alpha, \lambda)$	$\ln L(\mu, \sigma) = r(\ln 1 - \ln \sqrt{2\pi} - \ln \sigma) + \ln l - \sum_{i=1}^r \ln t_i - \frac{1}{2\sigma^2} \sum_{i=1}^r (\ln t_i - \varpi)^2 + (n-r) \ln \Phi(-z)$	$D_{EN} = \frac{\sum_{i=1}^n (x_i - \min x_i)}{\sqrt{n \sum_{i=1}^n (x_i - \bar{x})^2}}$	$D_{EN} < D_{EN}^*$
对数正态与威布尔	$LN(\mu, \sigma)$	$W(m, \eta)$	$D_{LW} = 2\pi e \sigma^2 \times \prod_{i=1}^n x_i f_w(x_i; m; \eta)$	$D_{LW} < D_{LW}$
	$W(m, \eta)$	$LN(\mu, \sigma)$	$D_{WLN} = (2\pi e \sigma^2)^{-\frac{1}{2}} \times [\prod_{i=1}^n x_i f_w(x_i; m; \eta)]^{-\frac{1}{n}}$	$D_{WLN} < D_{WLN}^*$

表 7-20 D_{NE}^* 临界值表

n	$\alpha = 0.01$		$\alpha = 0.05$		$\alpha = 0.10$	
	D_{NE}^*	$1 - \beta$	D_{NE}^*	$1 - \beta$	D_{NE}^*	$1 - \beta$
10	1.01	0.39	0.87	0.65	0.80	0.77
15	0.88	0.65	0.77	0.86	0.72	0.93
20	0.80	0.86	0.71	0.96	0.67	0.98
25	0.76	0.94	0.68	0.99	0.64	0.99
30	0.72	0.98	0.65	1.00	0.61	1.00

表 7-21 D_{NE}^* 临界值表

n	$\alpha = 0.01$		$\alpha = 0.05$		$\alpha = 0.10$	
	D_{NE}^*	$1 - \beta$	D_{NE}^*	$1 - \beta$	D_{NE}^*	$1 - \beta$
10	1.75	0.39	1.51	0.65	1.40	0.77
15	1.65	0.65	1.43	0.87	1.34	0.93
20	1.55	0.86	1.38	0.96	1.30	0.98
25	1.50	0.94	1.34	0.99	1.27	1.00
30	1.44	0.98	1.31	1.00	1.25	1.00

表 7-22 D_{LW}^* 临界值表

n	$\alpha = 0.01$		$\alpha = 0.05$		$\alpha = 0.10$		$\alpha=0.20$	
	D_{LW}^*	$1 - \beta$	D_{LW}^*	$1 - \beta$	D_{LW}^*	$1 - \beta$	D_{LW}^*	$1 - \beta$
20	1.144	0.22	1.082	0.48	1.038	0.61	1.015	0.75

(续表)

n	$\alpha = 0.01$		$\alpha = 0.05$		$\alpha = 0.10$		$\alpha = 0.20$	
	D_{LW}^*	$1 - \beta$	D_{LW}^*	$1 - \beta$	D_{LW}^*	$1 - \beta$	D_{LW}^*	$1 - \beta$
30	1.095	0.39	1.044	0.63	1.020	0.75	0.993	0.86
40	1.070	0.53	1.028	0.76	1.007	0.85	0.984	0.93
50	1.054	0.63	1.014	0.83	0.998	0.91	0.976	0.96

 表 7-23 D_{WLN}^* 临界值表

n	$\alpha = 0.01$		$\alpha = 0.05$		$\alpha = 0.10$		$\alpha = 0.20$	
	D_{WLN}^*	$1 - \beta$	D_{WLN}^*	$1 - \beta$	D_{WLN}^*	$1 - \beta$	D_{WLN}^*	$1 - \beta$
20	1.120	0.20	1.067	0.43	1.041	0.57	1.008	0.73
30	1.088	0.34	1.047	0.62	1.019	0.74	0.991	0.84
40	1.063	0.51	1.026	0.75	1.005	0.85	0.980	0.93
50	1.045	0.66	1.016	0.82	0.995	0.91	0.974	0.96

【例 7-11】从母体中抽取 $n=20$ 的子样, 得到其观察值。现以正态分布为原假设, 以指数分布为备择假设, 其统计量的计算过程如表 7-24 所示。

表 7-24 以正态分布为原假设, 以指数分布为备择假设的统计量计算

x_i	$X_i - \min x_i$	$x_i - \bar{x}$	$(x_i - \bar{x})^2$
35.15	8.31	-2.15	4.62
44.62	17.78	7.32	53.58
40.85	14.01	3.55	12.60
45.32	18.48	8.02	64.32
36.08	9.24	-1.22	1.49
38.97	12.13	1.67	2.79
32.84	6	-4.46	19.89
34.36	7.52	-2.94	8.64
38.05	11.21	0.75	0.56
26.84	0	-10.46	109.41
33.68	6.84	-3.62	13.10
42.90	16.06	5.6	31.36
33.57	6.73	-3.73	13.91
36.64	9.8	-0.66	0.44
33.82	6.98	-3.48	12.11

(续表)

x_i	$X_i - \min x_i$	$x_i - \bar{x}$	$(x_i - \bar{x})^2$
42.26	15.42	4.96	24.60
37.88	11.04	0.58	0.34
38.57	11.73	1.27	1.13
32.05	5.21	-5.25	27.56
41.50	14.66	4.2	17.64
$\bar{x} = 37.30$	10.46		
Σ	209.15		420.59

由表 7-24 可以得到:

$$D_{NE} = \frac{\sqrt{n \sum_{i=1}^n (x_i - \bar{x})^2}}{\sum_{i=1}^n (x_i - \min x_i)} = \frac{91.716}{209.15} = 0.44$$

查表得 D_{NE}^* 在 $\alpha=0.1$ 时为 0.67。由于 $D_{NE}=0.44 < D_{NE}^*=0.67$ ，所以接受此样本为正态分布的假设。

若以指数分布为原假设，正态分布为备择假设，则有 $D_{NE}=2.3$ ，查表，在 $\alpha=0.10$ 时有 $D_{NE}^*=1.3$ ，因为 $D_{NE}=2.3 > 1.3 = D_{NE}^*$ ，故拒绝此样本为指数分布的原假设。

除了用似然比检验法来鉴别不同分布类型外，统计学中还可以用各种分布函数的偏度与峰度之间的关系图形来鉴别其分布类型。

8. 数据分析中寿命分布的选择

在获得产品寿命试验的数据后，首先对数据进行探索性分析，使用直方图方法绘制失效率曲线以及分布密度曲线，并结合样本均值、标准差、偏度和峰度等常见的分布数字特征，进行分布的选择，然后再用拟合优度检验对数据是否来自所选择的总体分布进行判别。

7.7.2 分布参数估计

对于同一分布来说，分布参数不同，分布的概率密度曲线也就不同，因此在母体分布类型已经知道的情况下，数据分析的主要任务就是根据子样的统计数据来估计母体分布参数。由前述可知，指数分布只有一个参数，即失效率 λ ；正态分布有两个参数，均值 μ 及标准离差 σ ；对数正态分布也有两个参数，对数均值 μ 及对数

标准离差 σ ；而对于威布尔分布来说，则有 3 个分布参数，即形状参数 m ，尺度参数 t_0 或 η ，以及位置参数 γ 。只有既确定了产品的寿命分布类型，又掌握了产品的寿命分布参数以后，才能对产品的可靠性指标进行计算。

1. 分布参数的点估计

用一个点值来估计母体分布参数的方法，在统计学中称为参数的点估计法。如前所述，可以采用图估法来对分布参数进行点估计。此法的优点是简单易行，但其结果会因人而异，不甚精确。比较精确的点估计方法有矩法、最小二乘法 (LSQL)、极大似然法 (MLE)、最佳线性无偏估计法 (BLUE)、简单线性无偏估计法 (GLUE) 以及最佳线性不变估计法 (BLIE) 等。

根据矩法的原理，在 n 足够大时，将 n 次试验中事件 A 出现的频率 v_i/n 作为它出现的概率 p_i 的点估计值；将子样观察值的平均值：

$$\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i$$

作为母体数学期望 μ 的点估计值；将子样观察值的方差作为母体方差 σ^2 的点估计值等：

$$s_n^2 = \frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^2$$

关于矩法的内容请看有关数理统计方面的书籍。限于篇幅，下面只叙述在寿命试验数据统计分析中常用的最小二乘法 (LSQL)、极大似然法 (MLE)，其他的方法读者可参阅相关的资料。

(1) 最小二乘法 (LSQL)

最小二乘法是确定因变量与其自变量之间经验关系的一种估计方法。对于一次线性回归方程 $y = bx + a$ ，由试验观测值 (x_i, y_i) 可以得到系数 a 、 b 的点估计式：

$$\begin{cases} \hat{b} = \frac{\overline{xy} - \bar{x}\bar{y}}{\overline{x^2} - (\bar{x})^2} \\ \hat{a} = \bar{y} - \hat{b}\bar{x} \end{cases} \quad (7-30)$$

式中：

$$\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i$$

$$\bar{y} = \frac{1}{n} \sum_{i=1}^n y_i$$

$$\overline{x^2} = \frac{1}{n} \sum_{i=1}^n x_i^2$$



$$(\overline{x^2}) = \left(\frac{1}{n} \sum_{i=1}^n x_i^2 \right)$$

$$\overline{xy} = \frac{1}{n} \sum_{i=1}^n x_i y_i$$

在威布尔分布中, 若令 $x = \ln t$, $y = \ln \ln \frac{1}{1-F(t)}$, $B = \ln t_0$, 并设 $\gamma = 0$, 则经过直线化之后, 可以化为如下有线方程:

$$y = mx - B$$

因此, 若试验观察值为 $[t_i, F(t_i)]$ ($i=1, 2, \dots, n$), n 为试样数, 分别计算出 $x_i = \ln t_i$, $y_i = \ln \ln \frac{1}{1-F(t_i)}$ 以后, 由最小二乘法的系数公式可以得出:

$$\hat{m} = \frac{\overline{xy} - \bar{x}\bar{y}}{\overline{x^2} - (\bar{x})^2}$$

$$\hat{B} = \hat{m}\bar{x} - \bar{y}$$

由于 $B = \ln t_0$, 所以 $t_0 = e^B = e^{\hat{m}\bar{x} - \bar{y}}$, 故有:

$$\hat{n} = t_0^{1/\hat{m}} = e^{(\hat{m}\bar{x} - \bar{y})/\hat{m}} = e^{\bar{x}} / e^{\bar{y}/\hat{m}}$$

因此, 威布尔分布的形状参数 m 及特征寿命 η 的点估计值为:

$$\begin{cases} \hat{m} = \frac{\overline{xy} - \bar{x}\bar{y}}{\overline{x^2} - (\bar{x})^2} \\ \hat{\eta} = e^{\bar{x}} / e^{\bar{y}/\hat{m}} \end{cases} \quad (7-31)$$

(2) 极大似然法 (MLE)

极大似然法, 就是要选取使观察结果出现可能性为极大时的数值作为参数估计值的一种方法。步骤是先构造一个似然函数, 而后给出使似然函数取极大值的似然方程, 似然方程的解即为待估计参数的极大似然估计量。

假设有两个事件, 其中一个出现的概率为 0.99, 另一个为 0.01。显然, 在一次观察中人们趋于相信概率为 0.99 的那个事件。假定母体待估计的参数只有一个, 记为 θ 。我们在 θ 的一切值之中, 使得观察结果出现的概率最大的一个作为 θ 的估计值 $\hat{\theta}$ 。

假定母体具有由某一函数 $f(x, \theta)$ 表示的分布。 θ 是该母体的一个参数。现在, 设观测到的数据为 x_1, x_2, \dots, x_n , n 次独立观察得到的 n 个数据出现的概率, 便是各个数据出现概率的乘积:

$$f(x_1, x_2, \dots, x_n, \theta) = f(x_1, \theta) \cdot f(x_2, \theta) \cdots f(x_n, \theta)$$

把参数 θ 看成是子样 x_1, x_2, \dots, x_n 的函数, 则可以构造似然函数

$$L(\theta) = f(x_1, \theta)f(x_2, \theta) \cdots f(x_n, \theta)$$

使得 $L(\theta)$ 为最大的 θ 应满足方程:

$$\frac{dL(\theta)}{d\theta} = 0$$

由于 $L(\theta)$ 和 $\ln L(\theta)$ 的最大值是等价的, 为了计算的方便经常用如下方程来代替似然方程。

$$\frac{d \ln L(\theta)}{d\theta} = 0$$

似然方程 $\frac{dL(\theta)}{d\theta} = 0$ 或 $\frac{d \ln L(\theta)}{d\theta} = 0$ 的解, 就叫做参数 θ 的极大似然估计量。

下面以指数分布和正态分布为例, 采用极大似然估计法推导其参数估计公式。

① 指数分布平均寿命的极大似然估计公式。

在产品寿命服从指数分布时, 只有一个分布参数 λ , 由于指数分布的失效率 λ 与平均寿命 θ 之间有关系式 $\theta=1/\lambda$, 因而可以利用极大似然法计算产品平均寿命的点估计式。

寿命试验一般分为定数截尾和定时截尾两种方式, 每种情况又可分为有替换和无替换两种情况。以无替换定数截尾试验为例, 假设试样总数 n , 第 r 个产品失效时刻为 t_r , 则 r 个产品在单位时间内的失效概率为: $f(t_i, \theta)$ ($i=1, 2, \dots, t_r$)。

对于指数分布来说, 有 $f(t_i, \theta) = \frac{1}{\theta} e^{-\frac{t_i}{\theta}}$ 。不失效产品在 t_r 时不失效的概率应为 $R(t_r) = e^{-t_r/\theta}$ 。由于有 $n-r$ 个不失效, 故总的不失效概率应为 $e^{-t_r(n-r)/\theta}$ 。因此, 可以构造出似然函数为:

$$\begin{aligned} L(\theta) &= \frac{n!}{(n-r)!} \prod_{i=1}^r \left(\frac{1}{\theta} e^{-t_i/\theta} \right) \cdot (e^{-(n-r)t_r/\theta}) \\ &= \frac{n!}{(n-r)!} \left(\frac{1}{\theta} \right)^r \exp \left\{ - \left[\sum_{i=1}^r t_i + (n-r)t_r \right] / \theta \right\} \\ &= \frac{n!}{(n-r)!} \left(\frac{1}{\theta} \right)^r e^{-T_{r,n}/\theta} \\ \ln L(\theta) &= \ln \left(\frac{n!}{(n-r)!} \right) - r \ln \theta - T_{r,n}/\theta \\ \frac{\partial}{\partial \theta} \ln L(\theta) &= -\frac{r}{\theta} + \frac{1}{\theta^2} T_{r,n} = 0 \end{aligned}$$

由此解得:

$$\hat{\theta}_{r,n} = T_{r,n} / r \quad (7-32)$$

式中: $T_{r,n} = \sum_{i=1}^r t_i + (n-r)t_r$ 。

由此可以证明估计量 $\bar{\theta}_{r,n}$ 具有无偏性。

失效率 λ 的极大似然估计量应为

$$\hat{\lambda}_{r,n} = 1 / \hat{\theta}_{r,n} = r / T_{r,n}$$

可以证明估计量 $\hat{\lambda}_{r,n}$ 是有偏的, 因而进行修正后, 其无偏式为

$$\hat{\lambda}_{r,n} = \frac{r-1}{T_{r,n}} \quad (7-33)$$

无替换定时截尾试验、有替换定数截尾试验、有替换定时截尾试验等同于无替换定数截尾试验, 也可以得到类似的点估计公式, 所不同的是试验的总元件小数 $T_{r,n}$ 的含义不同。在各种不同情况下 $T_{r,n}$ 分别表示为:

$$T_{r,n} = \begin{cases} \sum_{i=1}^r t_i + (n-r)t_r & (n, r, \text{无替换}) \\ \sum_{i=1}^r t_i + (n-r)t_0 & (n, t_0, \text{无替换}) \\ nt_0 & (n, t_0, \text{有替换}) \\ nt_r & (n, r, \text{有替换}) \end{cases}$$

② 正态分布极大似然法的估计公式。

正态分布有两个分布参数, 即均值 μ 和方差 σ^2 。利用极大似然法可以求出其平均寿命及寿命方差的点估计式。假定从产品寿命服从正态分布的母体中随机抽取 n 个样品进行试验, 假设试验的观测值为 x_1, x_2, \dots, x_n , 则可以构造似然函数为

$$\begin{aligned} L(\mu, \sigma) &= \prod_{i=1}^n f(x_i, \mu, \sigma) = \prod_{i=1}^n \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}\left(\frac{x_i - \mu}{\sigma}\right)^2} \\ &= \left(\frac{1}{\sqrt{2\pi}\sigma}\right)^n e^{-\frac{1}{2\sigma^2}\left[\sum_{i=1}^n (x_i - \mu)^2\right]} \\ \ln L(\mu, \sigma) &= n \ln \left(\frac{1}{\sqrt{2\pi}\sigma}\right) - \frac{1}{2\sigma^2} \sum_{i=1}^n (x_i - \mu)^2 \\ &= n \ln 1 - n \ln \sqrt{2\pi} - n \ln \sigma - \frac{1}{2\sigma^2} \sum_{i=1}^n (x_i - \mu)^2 \end{aligned}$$

分别对 μ 、 σ 求偏导数，则有似然方程：

$$\begin{aligned}\frac{\partial \ln L(\mu, \sigma)}{\partial \mu} &= \frac{1}{\sigma^2} \sum_{i=1}^n (x_i - \mu) \\ &= \frac{1}{\sigma^2} \left[\sum_{i=1}^n x_i - n\mu \right] = 0\end{aligned}\quad (*)$$

$$\frac{\partial \ln L(\mu, \sigma)}{\partial \sigma} = -\frac{n}{\sigma} + \frac{1}{\sigma^3} \sum_{i=1}^n (x_i - \mu) = 0 \quad (**)$$

由 (*) 式可得到平均寿命方差的点估计式：

$$\hat{\mu} = \sum_{i=1}^n x_i / n \quad (7-34)$$

由 (**) 式可得到寿命方差的点估计式：

$$\hat{\sigma}^2 = \frac{1}{n} \sum_{i=1}^n (x_i - \hat{\mu})^2$$

可以证明， $\hat{\mu}$ 是 μ 的无偏估计量，而 $\hat{\sigma}^2$ 不是 σ^2 的无偏估计量， σ^2 的无偏估计量应该表示为

$$\hat{\sigma}^2 = \frac{1}{n-1} \sum_{i=1}^n (x_i - \hat{\mu})^2 \quad (7-35)$$

③ 估计量好坏的标准。

参数的估计量是一个随机变量，它一般是在母体参数值的附近波动，而不是母体的真实值。不仅采用同一估计式在不同的试验中会得到不同的结果，而且对于同一参数也可以有不同的点估计式。例如，可以用如下公式作为寿命方差的估计式。

$$\hat{\sigma}^2 = \frac{1}{n} \sum_{i=1}^n (t_i - \bar{t})^2$$

$$\hat{\sigma}^2 = \frac{1}{n-1} \sum_{i=1}^n (t_i - \bar{t})^2$$

为了判断估计量的好坏，通常对估计量还有无偏性、有效性及一致性等要求。所谓无偏性，即要求估计量 $\hat{\theta}$ 围绕 θ 摆动而不是偏离在参数真实值的一侧，也就是说要求没有系统性误差；所谓有效性，即要求 $\hat{\theta}$ 在 θ 附近的波动幅度要小，或者说 $\hat{\theta}$ 距离 θ 要小；所谓一致性，即要求随着样品个数 n 的增大， $\hat{\theta}$ 围绕 θ 摆动的幅度要越来越小。

严格来讲，如果估计量 $\hat{\theta}$ 的数学期望值就是参数的真实值，即 $E(\hat{\theta}) = \theta$ ，则称 $\hat{\theta}$ 是 θ 的无偏估计量。例如用子样的均值作为母体数学期望值的估计量是具有无偏性的，这是因为：若以 \bar{t} 来表示子样的均值，以 μ 来表示母体的数学期望，则由定义：

$$\bar{t} = \frac{\sum_{i=1}^n t_i}{n} \quad E(t) = \mu$$

可以得到:

$$E(\bar{t}) = E\left(\frac{\sum_{i=1}^n t_i}{n}\right) = \frac{1}{n} \sum_{i=1}^n E(t_i) = \frac{1}{n} \sum_{i=1}^n \mu$$

因此 \bar{t} 是 μ 的无偏估计量。

同样可以证明, 以如下公式作为寿命方差的估计量是具有无偏性的。

$$\hat{\sigma}^2 = \frac{1}{n-1} \sum_{i=1}^n (t_i - \bar{t})^2$$

假设 $\hat{\theta}_1$ 、 $\hat{\theta}_2$ 为参数 θ 的两个估计量。如果 $\hat{\theta}_1$ 在 θ 附近的离差比 $\hat{\theta}_2$ 在 θ 附近的离差要小, 也就是说, 若有:

$$E(\hat{\theta}_1 - \theta)^2 < E(\hat{\theta}_2 - \theta)^2 \text{ 或 } D[\theta_1] < D[\theta_2] \quad (7-36)$$

则称估计量 $\hat{\theta}_1$ 比估计量 $\hat{\theta}_2$ 更为有效。

参数估计量 $\hat{\theta}_n$ 是一个随机变量, 若当 $n \rightarrow \infty$ 时, $\hat{\theta}_n$ 依概率收敛于母体参数的真值 θ , 也就是说, 对于任意给定的 ε , 总有:

$$\lim_{n \rightarrow \infty} P(|\theta_n - \theta| < \varepsilon) = 1 \quad (7-37)$$

则称 θ_n 为 θ 的一致性估计量, 对于一致性估计量来说, 若观测的数据越多, 则由此所求的估计值 $\hat{\theta}$ 越接近于母体参数 θ 。

④ 最佳线性无偏估计 (BLUE) 法。

如果 $\hat{\theta}$ 是观测值的线性函数, 并且具有无偏性, 则称 $\hat{\theta}$ 是 θ 的线性无偏估计量。假如在 θ 的所有线性无偏估计量中 $\hat{\theta}$ 又具有方差最小的性质, 则称 $\hat{\theta}$ 是 θ 的最佳线性无偏估计量。求这种估计量的方法, 称为最佳线性无偏估计法, 简称为 BLUE 法。

⑤ 简单线性无偏估计 (GLUE) 法。

如果 $\hat{\theta}$ 是观测值的线性函数且具有无偏性, 并且是稍次于最佳线性无偏估计量的估计量, 则称 $\hat{\theta}$ 是 θ 的简单线性无偏估计量。求这种估计量的方法, 称为简单线性无偏估计法, 简称为 GLUE 法。

⑥ 最佳线性不变估计 (BLIE) 法。

假设随机变量的分布函数具有 $F(t) = G\left(\frac{t - \mu}{\sigma}\right)$ 的形式, 若以 θ 代表分布参数 μ 、 σ , 如果 θ 的估计量 $\hat{\theta}$ 是观测值的线性函数, 并且 $\hat{\theta}$ 的均方误差同尺度直平方

σ^2 的比值与参数 μ 、 σ 无关, 即 $E(\hat{\theta} - \theta)^2 / \sigma^2$ 是一个常数, 与 μ 、 σ 无关, 则称 $\hat{\theta}$ 是 θ 的线性不变估计量。如果在 θ 的所有线性不变估计量中, $\hat{\theta}$ 又具有均方误差 $E(\hat{\theta} - \theta)^2$ 最小的性质, 则称 $\hat{\theta}$ 是 θ 的最佳线性不变估计量。这种求估计量的方法, 称为最佳线性不变估计法, 简称为 BLIE 法。

可以证明, 对数威布尔分布参数 σ 和 μ 的 BLIE 估计公式为

$$\tilde{\sigma} = 2.3026 \sum_{j=1}^r C_I(n, r, j) \ln t_{j,n} \quad (7-38)$$

$$\tilde{\mu} = 2.3026 \sum_{j=1}^r D_I(n, r, j) \ln t_{j,n} \quad (7-39)$$

式中: $C_I(n, r, j)$ 称为 σ 的最好线性不变估计系数; $D_I(n, r, j)$ 称为 μ 的最好线性不变估计系数。关于它们的数值可根据 n , r 及次序 j 查专门的数表得到。

上述各种点估计方法的详尽论述和严格证明在概率统计及各种有关的文献资料中可以找到, 在此恕不多谈。为了应用的方便, 下面将上述的一些结果公式, 按分布类型分类, 归纳整理成表 7-25。

表 7-25 (a) 指数分布平均寿命参数的点估计公式

	无替换试验	有替换试验	符号说明
定时截尾	$\hat{\theta} = \sum_{i=1}^r t_i + (n-r)t_s / r$	$\hat{\theta} = \frac{nt_s}{r}$	n 为样本观察总数, r 为观察中的失效样品数, t_i 为第 i 号样品的失效时间, t_s 为截尾时间
定数截尾	$\hat{\theta} = \sum_{i=1}^r t_i + (n-r)t_r / r$	$\hat{\theta} = \frac{nt_r}{r}$	t_r 为定数截尾时间

表 7-25 (b) 双参数指数分布的点估计式

	无替换试验	有替换试验
定数截尾	$\hat{\theta}_{r,n} = \left[\sum_{i=1}^r (t_i - t_1) + (n-r)(t_r - t_1) \right] / r, \hat{\gamma} = t_1$	$\hat{\theta}_{r,n} = n(t_r - t_1) / r, \hat{\gamma} = t_1$
定时截尾	$\hat{\theta}_{r,n} = \left[\sum_{i=1}^r (t_i - t_1) + (n-r)(t_r - t_1) \right] / r, \hat{\gamma} = t_1$	$\hat{\theta}_{r,n} = n(t_s - t_1) / r, \hat{\gamma} = t_1$

表 7-25 (c) 正态分布参数的点估计式

方 法	位置参数	尺度参数	备 注
MLE 法	$\hat{\mu} = \frac{1}{n} \sum_{i=1}^n x_i$	$\hat{\sigma}^2 = \frac{1}{n-1} \sum_{i=1}^n (x_i - \bar{x})^2$	
BLUE 法	$\mu^* = \sum_{j=1}^r D(n, r, j) x_j$	$\sigma^* = \sum_{j=1}^r C(n, r, j) x_j$	Sarhan & Greenberg 给出了 $C(n, r, j)$ 、 $D(n, r, j)$ 表
BLIE 法	$\tilde{\mu} = \mu^* - \frac{B_{r,n}}{1 + l_{r,n}} \sigma^*$	$\tilde{\sigma} = \frac{\sigma^*}{1 + l_{r,n}}$	$l_{r,n}$ 和 $B_{r,n}$ 可查专用表



(续表)

方 法	位置参数	尺度参数	备 注
GLUE 法	$\mu^{**} = x_r - E(Z_r)\sigma^{**}$	$\sigma^{**} = \frac{(r-1)x_r - \sum_{i=1}^{r-1} x_i}{nk_{r,n}}$	$E(Z_r)$ 、 $nk_{r,n}$ 可查专用表, 适于 $r \leq 0.9n$ 的情况

表 7-25 (d) 对数正态分布的点估计式

方 法	位置参数	尺度参数	备 注
MLE	全子样 $\hat{\mu} = \frac{1}{n} \sum_{i=1}^n \ln t_i$	$\hat{\sigma}^2 = \frac{1}{n-1} \sum_{i=1}^n (\ln t_i - \hat{\mu})^2$	
	截尾情况 $\hat{\mu} = \bar{x} + (\hat{\sigma}^2 - s^2)/d$	$\hat{\sigma} = d/g(Z_S)$	$g(Z_S)$ 根据 $\frac{r}{n}$ 与 D 查表得到 $x_i = \ln t_i$ $\bar{x} = (1/r) \sum_{i=1}^r x_i$ $d = xs - \bar{x}$ $s^2 = (1/r) \sum_{i=1}^r (x_i - \bar{x})^2$ $D = \frac{d^2}{d^2 + s^2}$
BLUE 法	$\mu^* = \sum_{j=1}^r D(n, r, j) \ln t_j$	$\sigma^* = \sum_{j=1}^r C(n, r, j) \ln t_j$	$C(n, r, j)$ 、 $D(n, r, j)$ 可查专用表
BLIE 法	$\tilde{\mu} = \mu^* - \frac{B_{r,n}}{1 + l_{r,n}} \sigma^*$	$\tilde{\sigma} = \frac{\sigma^*}{1 + l_{r,n}}$	$B_{r,n}$ 和 $l_{r,n}$ 可查专用表
GLUE 法	$\mu^{**} = \ln t_r - E(Z_r)\sigma^{**}$	$\sigma^{**} = \frac{(r-1) \ln t_r - \sum_{i=1}^{r-1} \ln t_i}{nk_{r,n}}$	$E(Z_r)$ 、 $nk_{r,n}$ 可查专用表

表 7-25 (e) 威布尔分布的点估计式

方 法	形状参数	尺度参数
LSQL	$\hat{m} = \frac{\overline{xy} - \bar{x} \bar{y}}{\bar{x}^2 - \bar{x}^2}$	$\hat{\eta} = e^{\bar{x}} / e^{\bar{y}/\hat{m}}$
MLE	全子样 $\hat{m} = \eta^m / (t^m x - \eta^m t \cdot \bar{x})$	$\hat{\eta} = (\bar{t}^m)^{1/m}$
	截尾情况 $\hat{m} = \frac{\eta^m \cdot r}{\sum_{i=1}^r t_i^m \ln t_i + (n-r) t_r^m \ln t_r - \eta^m \sum_{i=1}^r \ln t_i}$	$\hat{\eta} = \left(\frac{1}{r} \left[\sum_{i=1}^r t_i^m + (n-r) t_r^m \right] \right)^{1/m}$

表 7-25 (f) 极值分布与威布尔分布的点估计式

方 法	尺度参数	位置参数	形状参数
BLUE	$\hat{\sigma} = \sum_{j=1}^r C(n, r, j) \ln t_j$	$\hat{\mu} = \sum_{j=1}^r D(n, r, j) \ln t_j$	$\hat{m} = g_{r,n} / \hat{\sigma}$
BLIE	$\hat{\sigma} = \sum_{j=1}^r C_l(n, r, j) \ln t_j$	$\hat{\mu} = \sum_{j=1}^r D_l(n, r, j) \ln t_j$	$\hat{m} = g_{r,n} / \hat{\sigma}$
GLUE	$\hat{\sigma} = \frac{(r-1) \ln t_r - \sum_{i=1}^{r-1} \ln t_i}{nk_{r,n}}$	$\hat{\mu} = \ln t_r - \hat{\sigma} E(Z_r)$	$\hat{m} = g_{r,n} / \hat{\sigma}$
备注	$C(n, r, j)$ 、 $D(n, r, j)$ 、 $D_l(n, r, j)$ 、 $C_l(n, r, j)$ 、 $E(Z_r)$ 、 $nk_{r,n}$ 、 $g_{r,n}$ 可查专用表		

2. 分布参数的区间估计

分布参数的估计除了点估计以外，为了准确地说明估计量在 θ 附近的变化范围，还可进行区间估计。若子样的函数 θ_L 和 θ_U ，使得未知参数 θ 落在区间 $[\theta_L, \theta_U]$ 内的概率为 $(1-\alpha)$ ，即

$$P(\theta_L \leq \theta \leq \theta_U) = 1 - \alpha$$

其中 $\theta < \alpha < 1$ ， $1-\alpha$ 称为置信度， α 称为显著水平，则称区间 $[\theta_L, \theta_U]$ 为置信度为 $1-\alpha$ 的置信区间， θ_L 为置信下限， θ_U 为置信上限。

置信区间的构造原理，牵涉到较多的数理统计知识。构造置信区间的基本方法一般有两种：一种是找出子样 x_1, x_2, \dots, x_n 和参数 θ 的函数 y ，如果 y 的概率分布已知，而且与 θ 无关，那么就可以得到两个常数 a, b ，使得 $P(\theta_L \leq \theta \leq \theta_U) = 1 - \alpha$ ，再把事件 $a \leq y \leq b$ 换成与之相等的事件 $\theta_L \leq \theta \leq \theta_U$ ，就得到 $P(\theta_L \leq \theta \leq \theta_U) = 1 - \alpha$ ，从而得到 θ 的置信水平为 $1-\alpha$ 的置信区间。

例如母体服从正态分布 $N(\mu, \sigma)$ ，当 σ 已知时，可以构造一个统计量 $y = \frac{\sum_{i=1}^n x_i}{n} - \mu$ ，显然它是子样 x_1, x_2, \dots, x_n 和待估参数 μ 的函数。由概率统计学

的中心极限定理可知， $\frac{\bar{x} - \mu}{\sigma/\sqrt{n}}$ 是渐近于标准正态分布 $N(0,1)$ 的，而 $N(0,1)$ 是与待估参数无关的，因此有 $P\left(\left|\frac{\bar{x} - \mu}{\sigma/\sqrt{n}}\right| \leq U_\alpha\right) = 1 - \alpha$ ，其中 U_α 是正态分布的双侧 α 分位点。由此可见，有：

$$P\left(-U_\alpha \leq \frac{\bar{x} - \mu}{\sigma/\sqrt{n}} \leq U_\alpha\right) = 1 - \alpha$$



$$P\left(\bar{x} - U_{\alpha} \frac{\sigma}{\sqrt{n}} \leq \mu \leq \bar{x} + U_{\alpha} \frac{\sigma}{\sqrt{n}}\right) = 1 - \alpha$$

最后得到:

$$\mu_L = \bar{x} - \frac{\sigma}{\sqrt{n}} U_{\alpha}, \quad \mu_U = \bar{x} + \frac{\sigma}{\sqrt{n}} U_{\alpha} \quad (7-40)$$

这就是正态分布平均寿命的区间估计公式。

又如对于指数分布的定数截尾试验, 可以构造统计量 $y = 2\lambda T_{r,n} = \frac{2r\hat{\theta}}{\theta}$ 。可以证明, $2\lambda T_{r,n}$ 是服从 $x_{\alpha}^2(2r)$ 分布的, 因此有关系式:

$$\frac{x_{\alpha}^2(2r)}{2} \leq 2\lambda T_{r,n} \leq \frac{x_{1-\alpha}^2(2r)}{2}$$

最后得到定数截尾试验的区间估计式为:

$$P\left(\frac{x_{\alpha}^2}{2T_{r,n}} \leq \lambda \leq \frac{x_{1-\alpha}^2(2r)}{2T_{r,n}}\right) = 1 - \alpha \quad (7-41)$$

求信置区间的另一种方法是: 设待估计参数 θ 的估计量为 $\theta = t(x_1, x_2, \dots, x_n)$ 。这是一个随机量, 通常可取极大似然估计量, 假设它的密度函数为 $g(t', \theta)$, t' 是 $t(x_1, x_2, \dots, x_n)$ 的一个观察值, 即从母体抽得一个子样 x_1, x_2, \dots, x_n 后函数 $t(x_1, x_2, \dots, x_n)$ 的值。把 θ 作为未知数, 解方程组:

$$\int_{t'}^{\infty} g(t', \theta) dt = \frac{\alpha}{2}$$

$$\int_{-\infty}^{t'} g(t', \theta) dt = \frac{\alpha}{2}$$

便可得到信置区间的下限 θ_L 和上限 θ_U 。

总之, 参数的区间估计是对未知数参数 θ 给出一个估计范围 (θ_L, θ_U) , 其中 θ_L 和 θ_U 是通过子样观察值, 由数理统计方法推算出来的。

常见的区间估计公式见表 7-26。

【例 7-12】 对 20 个电阻器进行 3000 小时的 120℃ 的高温试验, 其中失效 12 个, 失效时刻分别为: 270、420、500、920、1380、1510、1650、1760、2100、2320、2350、2650 (小时)。

假定该电阻器的失效服从指数分布, 试求其平均寿命 θ 的点估计及区间估计值 ($\alpha=0.2$)。

表 7-26 双边区间估计公式

分 布		区间估计式	备 注
指数分布	定数	$P\left(\frac{\chi_{a/2}(2r)}{2T} \leq \lambda \leq \frac{\chi_{1-a/2}^2(2r)}{2T}\right) = 1-a$	$r=1,2,\dots,n$; $\chi_y^2(n)$ 为下侧分位数表
	定时	$P\left(\frac{\chi_{a/2}^2(2r)}{2T} \leq \lambda \leq \frac{\chi_{1-a/2}^2(2r+2)}{2T}\right) = 1-a$ $P\left(\frac{\chi_{a/2}^2(2n)}{2T} \leq \lambda \leq \frac{\chi_{1-a/2}^2(2n)}{2T}\right) = 1-a$	$r=0,1,2,\dots,n-1$ 时 $r=n$ 时
	只知失效时	$P\left\{ \ln\left[1 + \left(\frac{r}{n-r+1}\right)F_{a/2}(2r, 2n-2r+2)\right] / t_s \leq \lambda \leq \ln\left[1 + \left(\frac{r+1}{n-r}\right)F_{1-a/2}(2r+2, 2n-2r)\right] / t_s \right\} = 1-a$	$F\gamma(n_1, n_2)$ 为 F 分布的下侧分位数表
正态分布	μ 的估计	$P\left[\hat{\mu} + \frac{\sigma}{\sqrt{n}}u_{a/2} \leq \mu \leq \hat{\mu} + \frac{\sigma}{\sqrt{n}}u_{1-a/2}\right] = 1-a$ $P\left[\hat{\mu} + \frac{\sigma}{\sqrt{n}}t_a(n-1) \leq \mu \leq \hat{\mu} + \frac{\sigma}{\sqrt{n}}t_a(n-1)\right] = 1-a$	σ 已知时, u_γ 为正态分位数表; σ 未知时, $t_\gamma(n)$ 为 t 分位数表
	σ 的估计	$P\left[\frac{(n-1)\hat{\sigma}^2}{\chi_{1-a/2}^2(n-1)} \leq \sigma^2 \leq \frac{(n-1)\hat{\sigma}^2}{\chi_{a/2}^2(n-1)}\right] = 1-a$	
对数正态分布	MLE 法	$P\left[\hat{\mu} - \frac{\hat{\sigma}}{\sqrt{n-1}}t_a(n-1) \leq \mu \leq \hat{\mu} + \frac{\hat{\sigma}}{\sqrt{n-1}}t_a(n-1)\right] = 1-a$ $P\left[\frac{n\hat{\sigma}^2}{\chi_{1-a/2}^2(n-1)} \leq \sigma^2 \leq \frac{n\sigma^2}{\chi_{a/2}^2(n-1)}\right] = 1-a$	
	BLUE 法	$P\left[\hat{\mu} - \frac{\hat{\sigma}}{\sqrt{n}}t_a(n-1) \leq \mu \leq \hat{\mu} + \frac{\hat{\sigma}}{\sqrt{n}}t_a(n-1)\right] = 1-a$ $P\left[\frac{(n-1)\hat{\sigma}^2}{\chi_{1-a/2}^2(n-1)} \leq \sigma^2 \leq \frac{(n-1)\hat{\sigma}^2}{\chi_{a/2}^2(n-1)}\right] = 1-a$	
	MLE 法	$P\left[\frac{\hat{m}}{z_{1-a/2}} < m < \frac{\hat{m}}{z_{a/2}}\right] = 1-a$ $P\left[\hat{\eta}e^{-\frac{\eta_{1-a/2}}{\hat{m}}} < \mu < \hat{\eta}e^{-\frac{\eta_{1-a/2}}{\hat{m}}}\right] = 1-a$	Z_γ 、 V_γ 可查专用数表, 适用于全子样
		$P[\hat{m} - u_{a/2}\hat{\sigma}_m < m < \hat{m} + u_{a/2}\hat{\sigma}_m] = 1-a$ $P[\hat{\eta}e^{-u_{a/2}\hat{\sigma}_\mu} < \eta < \hat{\eta} + \hat{\eta}e^{u_{a/2}\hat{\sigma}_\mu}] = 1-a$	μ_γ 可查标准正态分布表, 适用于截尾试验



(续表)

分 布		区间估计式	备 注
威 布 尔 分 布	BLUE 法	$P\left[\frac{(1+I_{r,n})w_{a/2}}{\sigma^*} \leq m \leq \frac{(1+I_{r,n})w_{1-a/2}}{\sigma^*}\right] = 1-a$ $P\left[\mu^* - \frac{B_{r,n}\sigma^*}{1+I_{r,n}} - \frac{\sigma^*}{1+I_{r,n}}v_{0.368,a/2} \leq \eta \leq \mu^* - \frac{B_{r,n}\sigma^*}{1+I_{r,n}} - \frac{\sigma^*}{1+I_{r,n}}v_{0.368,1-a/2}\right] = 1-a$	$w_a, B_{r,n}, I_{r,n}$ 查专用数 表, $v_{0.368} = \frac{\tilde{\mu} - \mu}{\tilde{\sigma}}$ 查专用数 表, 适用于定数截尾 $n > 25$ 的情况
	BLIE 法	$P[w_{a/2}/\tilde{\sigma} \leq m \leq w_{1-a/2}/\tilde{\sigma}] = 1-a$ $P[\tilde{\mu} - \tilde{\sigma}V_{0.368,1-a/2} \leq \ln\eta \leq \tilde{\mu} - \tilde{\sigma}V_{0.368,a/2}] = 1-a$	
		$P\left[\frac{I_{r,n}\chi^2_{a/2}(2/I_{r,n})}{2\sigma^{**}} \leq m \leq \frac{I_{r,n}\chi^2_{1-a/2}(2/I_{r,n})}{2\sigma^{**}}\right] = 1-a$	
	GLUE 法	$P\left[\ln t_s - \sigma^{**} \ln \ln \frac{1}{\beta_{a/2}(n-s+1, s)} \leq \ln \eta \leq \ln t_s - \sigma^{**} \ln \ln \frac{1}{\beta_{1-a/2}(n-s+1, s)}\right] = 1-a$ $P\left\{\mu^{**} + \frac{B_{r,n}}{1_{r,n}}[F_{1-a/2}(f_1, f_2) - 1] \sigma^{**} \leq \ln \eta \leq \mu^{**} + \frac{B_{r,n}}{1_{r,n}}[F_{a/2}(f_1, f_2) - 1] \sigma^{**}\right\} = 1-a$ <p>式中: $f_1 = 2B_{r,n}/1_{r,n}(A_{r,n}1_{r,n} - B_{r,n}^2)$ $f_2 = 2/1_{r,n}$</p>	适用于 $n \geq 15$ 、 $r/n \geq 0.4$ 的情况 适用于 $n \leq 25$ 、 $\frac{r}{n} \leq 0.5$ 的情况

解:
$$T = \sum_{i=1}^{12} t_i + (n-r)t_s = 17832 + 8 \times 3000 = 41830 \text{ (小时)}$$

因此:

$$\hat{\theta} = \frac{T}{r} = \frac{41830}{12} = 3486 \text{ (小时)}$$

按区间估计公式其下限值 θ_L 为

$$\theta_L = \frac{2T}{x_{2r+2, 1-\alpha/2}} = \frac{2 \times 41830}{x_{26, 0.9}} = \frac{2 \times 41830}{35.56} = 2353 \text{ (小时)}$$

θ_U 为

$$\theta_U = \frac{2T}{x_{2r, \alpha/2}} = \frac{2 \times 41830}{15.66} = 5342 \text{ (小时)}$$

以上给出的置信区间, 既有置信上限 θ_U 又有置信下限 θ_L , 这种置信区间称为

双边置信区间。如果只求 θ 的置信下限或置信上限，即：

$$P(\theta_L \leq \theta) = 1 - \alpha \text{ 或 } P(\theta \leq \theta_U) = 1 - \alpha$$

则置信区间 (θ_L, ∞) 与 $(-\infty, \theta_U)$ 叫做置信水平为 $1 - \alpha$ 的单边置信区间， θ_L 、 θ_U 分别叫做单边置信下限和单边置信上限。

以指数分布为例，把其单边区间估计式列于下表 7-27 中。

表 7-27 指数分布的单边区间估计式

	平均寿命下限 θ_L	失效率上限 λ_U
定时截尾	$\frac{2T}{\chi^2_{2r+2,1-\alpha}}$	$\frac{\chi^2_{2r+2,1-\alpha}}{2T}$
定数截尾	$\frac{2T}{\chi^2_{2r,1-\alpha}}$	$\frac{\chi^2_{2r,1-\alpha}}{2T}$

【例 7-13】 服从指数分布的某电台，在其产品说明书上要求 MTBF 达到 3000 小时，现从中随机抽取 5 台进行寿命试验。在不发生一次故障的条件下，最少试验多少小时才算合格（取置信度 90%）？

解：由平均寿命的下限估计式可知：

$$\theta_L \geq \frac{2T}{\chi^2_{2r+2,1-\alpha}}$$

所以，有：

$$\begin{aligned} \theta_L \chi^2_{2r+2,1-\alpha} &= 2T \\ \therefore T &= \frac{\theta_L \chi^2_{2r+2,1-\alpha}}{2} = \frac{3000 \chi^2_{2,0.9}}{2} = \frac{3000 \times 4.61}{2} = 6915 \end{aligned}$$

因此，需要有将近 7000 小时的总试验时间，如果以 5 台进行试验，则需要试验 $7000/5=1400$ 小时，也就是说，需要取 5 部电台进行 1400 小时的试验，不允许出现一次故障，才算产品合格。

3. 分布参数的检验

在试验结果的分析中，有时需要比较两批产品之间是否有变化，或者需要判断一批产品能否满足原定的标准，这时可以先对所研究的问题给出假设，例如假设两批产品之间无显著变化，假定一批新产品能满足某一标准，然后选取适当的统计量对原定的假设进行判断，这就是分布参数的假设检验问题。

假设检验的基本思想是：先对所研究的问题进行一原假设。根据具体情况构成一个合适的统计量，同时还必须了解这一统计量在原假设正确时的精确分布或渐近分布，然后按照一定的置信度确定拒绝或接受的标准，这样就构成了检验法。

对于正态分布参数进行假设检验时，通常有 u 检验法、 t 检验法、 F 检验法和 χ^2 法等等， u 检验法是构造一个服从正态分布或渐近于正态分布的 u 统计量，在母体方差已知的情况下，检验一母体的 μ 或比较母体的 μ ，可用 u 检验法。 t 检验法是构造一个趋于 t 分布的 t 统计量，在方差未知，但能知道 $\sigma_1^2 = \sigma_2^2$ 的情况下可用 t 检验法来比较两母体的 μ 。 F 检验法是构造一个趋于 F 分布的 F 统计量，在方差未知的情况下，可用 F 检验法来比较两母体 σ^2 。 χ^2 分布的 χ^2 统计量，在母体 μ 已知或未知的情况下，可用 χ^2 检验法来检验母体的方差是否满足某一给定方差要求。

关于正态分布参数检验方法的应用条件及统计量表达形式如表 7-28（a）、（b）表示。关于威布尔分布参数检验方法的应用条件及统计量如表 7-28（c）所示。关于指数分布参数的检验方法如表 7-28（d）所示。除了表中列出的各种检验方法之外，还有巴特利特（Bartlett）检验法等。关于这些检验法的详细内容请参阅数量统计方面的有关资料。

表 7-28（a） 判断均值方差是否满足原定标准的检验

条 件	已知 σ^2	未知 σ^2	已知 μ	未知 μ
假设 H_0	$\mu = \mu_0$	$\mu = \mu_0$	$\sigma^2 \leq \sigma_0^2$	$\sigma \leq \sigma_0^2$
统计量 u	$\frac{\bar{x} - \mu_0}{\sigma / \sqrt{n}}$	$\frac{\bar{x} - \mu_0}{S / \sqrt{n}}$	$\frac{1}{\sigma_0^2} \sum (x_i - \mu)^2$	$\frac{1}{\sigma_0^2} \sum (x_i - \bar{x})^2$
u 的分布	$N(0,1)$	$t(n-1)$	$\chi^2(n)$	$\chi^2(n-1)$
否定域	$ u \geq u_\alpha$	$ u \geq t_{n-1, \alpha}$	$\mu \geq \chi_{n,1-\alpha}$	$u \geq \chi_{n-1,1-\alpha}$
查 表	查正态分布 α 的双侧分位数表	T 分布 α 的双侧分位数表	χ^2 分布 α 的下侧分位数表	χ^2 分布的下侧分位数表

表 7-28（b） 判断两母体参数是否有显著性差异的检验

条 件	已知 $\sigma_1^2、\sigma_2^2$	已知 $\sigma_1^2 = \sigma_2^2$ （但其值未知）	无
假设 H_0	$\mu_1 = \mu_2$	$\mu_1 = \mu_2$	$\sigma_1^2 = \sigma_2^2$
统计量 u	$\frac{x_1 - x_2}{\sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}}}$	$\frac{(\bar{x}_1 + \bar{x}_2)\sqrt{n_1 + n_2 - 2}}{\sqrt{(n_1 - 1)S_1^2 + (n_2 - 1)S_2^2} + \sqrt{\frac{1}{n_2} + \frac{1}{n_2}}}$	$\frac{S_1^2}{S_2^2}$
u 的分布	$N(0,1)$	$t(n_1 + n_2 - 2)$	$F(n_1 - 1, n_2 - 1)$
否定域	$ u \geq u_\alpha$	$ u \geq t_\alpha(n_1 + n_2 - 2)$	$u \geq F_{\alpha/2}(n_1 - 1, n_2 - 1)$ $u \leq [F_{\alpha/2}(n_1 - 1, n_2 - 1)]^{-1}$
查 表	正态分布 α 的双侧分位数表	T 分布 α 的双侧分位数表	F 分布的上侧分位数表
注： $\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i$ ； $S^2 = \frac{1}{n-1} \sum_{i=1}^n (x_i - \bar{x})^2$			

表 7-28 (c) 威布尔分布的参数检验

条 件	$n_1 = n_2 = \cdots = n_k$ $r_1 = r_2 = \cdots = r_k$	$n_1 = n_2 = \cdots = n_k$ $r_1 = r_2 = \cdots = r_k$	GLUE 或 BLUE
假设 H_0	$m_1 = m_2 = \cdots = m_k$	$\chi_{p1} = \chi_{p2} = \cdots = \chi_{pk}$	$m_1 = m_2 = \cdots = m_k$ 或 $\sigma_1 = \cdots = \sigma_k$
统计量	$W(r, n, k) = \frac{\hat{m}_k}{\hat{m}_1}$	$t(r, n, k, p) = \frac{\bar{m} \ln \frac{\hat{\chi}_p(k)}{\hat{\chi}_p(1)}}{\hat{\chi}_p(1)}$	B^2/C
否定域	$W(r, n, k) \geq W_{0.9}(r, n, k)$	$t(r, n, k, p) \geq t_{0.9}(r, n, k, p)$	$B^2/C \geq \chi^2_{1-\alpha}(k-1)$
备 注	$W_{0.9}(r, n, k)$ 查专用表	$t_{0.9}(r, n, k, p)$ 查专用表	巴特利特检验见相关资料

表 7-28 (d) 指数分布的参数检验

假设 H_0	统计量	否定域	备 注
$r_1 = r_2$	$T = \frac{(r_1 + r_2 - 2) x_1 - y_1 }{(r_1 - 1)\theta_1^* + (r_2 - 1)\theta_2^*}$	$T > C$	C 查专用表, C 与 n_1 及 d 有关, $d = r_1 + r_2 - 2$
$\theta_1 = \theta_2$	$F = \frac{T_1 r_2}{T_2 r_1}$	$F \geq F_{1-\alpha}(k-1)$	查 F 分布表
$\theta_1 = \theta_2$ $= \cdots = \theta_k$	$\frac{B_2}{C}$	$\frac{B_2}{C} \geq \chi^2_{1-\alpha}(K-1)$	巴特利特检验
来自同分布	$U = \frac{\max\{T_1, T_2, \cdots, T_K\}}{\min\{T_1, T_2, \cdots, T_K\}}$	$U \geq U_{0.5}(k, 2r)$	$U_{0.5}(k, 2r)$ 查专用表

【例 7-14】 某灯泡的寿命服从正态分布 $N(\mu, \sigma)$ ，并已知其平均寿命 $\mu=1100$ 小时，标准离差 $\sigma=200$ 小时。为了提高该灯泡质量，工厂进行了技术改革，现从新生产的灯光中抽出 20 只进行寿命试验，其寿命值分别为：1015、1072、1100、1123、1145、1156、1170、1175、1190、1196、1205、1212、1220、1238、1245、1260、1269、1277、1290、1360（小时），要求根据所得数据，判断产品的平均寿命是否有所提高。

解：这是一个需要对产品分布参数 μ 进行假设检验的问题。检验可按如下步骤进行：

- ① 给出假设，假定技术改革后产品的平均寿命没有提高，即 $H_0: \mu = \mu_0$ 。
- ② 选取统计量：查表 7-28 选取统计量 $u = \frac{x - \mu_0}{\sigma / \sqrt{n}}$ 。
- ③ 确定统计量的分布：由中心极限定理可知 $u = \frac{x - \mu_0}{\sigma / \sqrt{n}}$ 是服从标准正态分布 $N(0,1)$ 的。
- ④ 给定置信度 $1-\alpha$ ，令 $\alpha=0.05$ 。
- ⑤ 确定判断标准 u_α ，查标准正态分布 α 的双侧分位数据表得 $u_{0.05}=1.96$ 。
- ⑥ 计算统计量的观察值：

$$u = \frac{\bar{x} - \mu_0}{\sigma / \sqrt{n}} = \frac{1195.9 - 1100}{200 / \sqrt{20}} \\ = \frac{95.9 \times 4.472}{200} = 2.14$$

⑦ 给出判断：因为 $2.14 > 1.96$ ，所以有 $u \geq u_\alpha$ ，这就是说存在有 $P(|u| \geq u_\alpha = 0.05)$

因为 $|u| \geq u_\alpha$ 是小概率事件，小概率事件在一次试验中是很少发生的，现在偏偏发生，所以应该否定原假设，即原假设“技术改革后平均寿命没有提高”是不可信的。检验结果表明：有 95% 的置信度相信技术改革后平均寿命是有所提高的。

7.7.3 贝叶斯方法在可靠性数据分析中的应用

经典可靠性理论目前已经得到了广泛的应用，但是必须充分认识到，只有在大样本的前提条件下，用“故障频率”代替“故障概率”去表征产品可靠性才合理。然而对于大多数实际工程问题，用大样本数据作为前提假设是不切实际的，因此，经典可靠性理论在实际的工程应用中存在一定的局限性。为了解决实际工程应用中的一些小样本量问题，一般采用贝叶斯方法，利用经验信息得出“先验分布”，根据先验分布和试验数据得出后验分布，根据后验分布得出贝叶斯点估计和区间估计。

贝叶斯公式也称为逆概公式，描述的是事件 B 能且仅能与 A_1, A_2, \dots, A_n 中的任一个同时发生，并且知道 A_i 及 B 在事件 A_i 条件下发生的概率，那么能够得出 A_i 在 B 条件下发生的概率（后验概率）。

$$P(A_i | B) = \frac{P(A_i)P(B | A_i)}{\sum_{j=1}^N p(A_j) P(B | A_j)} \quad (7-42)$$

下面从随机变量的密度函数来描述贝叶斯公式。在贝叶斯统计中，密度函数记为 $p(x | \theta)$ ，表示在随机变量 θ 给定某个值时，总体指标 X 的条件分布。

① 根据 θ 的先验信息确定 θ 的先验分布 $\pi(\theta)$ 。

② 产生样本 $X = (x_1, \dots, x_n)$ 。设想从先验分布 $\pi(\theta)$ 中产生参数 θ ，在给定 θ 下，从总体分布 $p(x | \theta)$ 中产生一个样本 $X = (x_1, \dots, x_n)$ ，得到似然函数：

$$p(X | \theta) = \prod_{i=1}^n p(x_i | \theta)$$

③ 样本 x 和参数 θ 的联合分布为

$$h(X, \theta) = p(X | \theta) \pi(\theta)$$

④ 对未知参数 θ 进行推断，在没有样本信息的情况下，只能根据先验分布

$\pi(\theta)$ 对 θ 做出推断。在有样本的情况下, 可根据联合分布 $h(\theta|X)$ 对 θ 做出推断, 因此, 需要将 $h(\theta|X)$ 进行如下分解:

$$h(X, \theta) = h(\theta|X)m(X)$$

其中 $m(X)$ 是 X 的边缘密度函数:

$$m(X) = \int_{\Theta} h(X, \theta) d\theta = \int_{\Theta} p(X|\theta)\pi(\theta) d\theta$$

即它与 θ 无关, 其中 Θ 是 θ 的取值空间。

⑤ 因此可用 $h(\theta|X)$ 条件分布对 θ 做出推断, 得出贝叶斯公式的密度函数形式:

$$h(\theta|X) = \frac{h(X, \theta)}{m(X)} = \frac{p(X|\theta)\pi(\theta)}{\int_{\Theta} p(X|\theta)\pi(\theta) d\theta} \quad (7-43)$$

在给定样本 X 的情况下, θ 的条件分布被称为 θ 的后验分布。

得到后验分布 $h(\theta|X)$, 就能够集总体信息、样本信息和先验信息于一体, 全面描述参数 θ 的概率分布, 因此有关参数 θ 的点估计、区间估计、假设检验等也都可以从后验分布中提取相关信息。

7.8 可靠性数据库

7.8.1 概述

可靠性基础数据的缺乏是制约开展可靠性工作的瓶颈, 建立可靠性数据库系统, 收集和积累可靠性数据, 是开展一切可靠性工作的基础。

- 美国政府与工业界数据交换网 (GIDEP)
- 美国失效率数据交换网 (FARADA)
- 美国可靠性信息分析中心 (RIAC)
- 中国电子五所可靠性数据中心 (CEPREI_RDC)

本节介绍几个典型的可靠性数据库应用系统。

7.8.2 GIDEP

1. GIDEP 概述

美国的政府工业界数据交换网 (GIDEP) 组织开始建立于 1959 年, 当时为各军

兵种数据交换网 (the Interservice Data Exchange Program, IDEP)。最初只是为了减少重复试验、通过试验数据和技术信息的交换实现相似或相同产品的评价, 后来才扩展到其他任务系统甚至整个国防系统。

如今, GIDEP 是政府和工业界寻求减少资源消耗的合作行为, 主要是通过共享在研究、设计、开发、生产和系统、设备寿命周期工作阶段的技术信息来实现这种合作。

自 GIDEP 成立以来, 通过 GIDEP 数据库的使用和信息交换, 已报告节约了超过十亿的花费。GIDEP 数据正确的使用可在本质上改善采购和后勤阶段系统和元器件的质量及可靠性, 并减少复杂系统和设备的研发、制造费用。

该项目由美国政府资助, 由联邦后勤指挥部特许成立。GIDEP 受美国陆军、海军和空军, 以及 NASA、能源部、国防合同管理处、加拿大国防部、国防后勤处支持, 是美国管理和预算办公室 (OMB) 指定的接收和分发非一致性产品和材料信息的中心数据库, 是美国国防部指定的 DMSMS (制造源萎缩和材料短缺) 中心数据库, 并且有超过 2200 家的团体加入了该项目, 其中工业公司超过 1800 家, 超过 6500 家用户。按美国国防后勤处的 2010 财年预算, GIDEP 将获得 340 万的专项经费。

符合下列要求的方可成为 GIDEP 会员:

- 直接或间接给美国政府或加拿大国防部供应产品或提供服务的组织。
- 美国或加拿大政府部门、代表处或活动机构。
- 获许可的美国公共事业公司。

2. GIDEP 提供的数据信息

(1) DMSMS 数据 (发布停产断档信息)

有近 100 个供应商和 OEM 向 GIDEP 递交产品信息数据 (包括 DMSMS 数据, 大部分信息来源于供应商和 OEM), GIDEP 也通过 DSCC、DMSMS 技术中心 (DTC)、国防后勤信息服务部 (DLIS) 及 GIDEP 参与者发布 DMSMS 信息。到 2008 年止, DMSMS 数据量已经接近 50 万。

(2) 工程数据

工程数据提供下列材料的技术报告: 研究材料、质量评估、工程试验、非标准部件数据、元器件和材料规范、制造、设计、过程控制、可焊性数据, 以及元器件、部件、材料和工艺的其他相关工程数据。报告适用于商业和军事应用, 由于它覆盖范围宽, 因此将其分成 7 个目录: 工程报告 (ER)、管理报告 (MR)、试验报告 (TR)、非标准部件数据 (NP)、工艺规范 (PS)、焊接技术 (STL)、计算机技术文档 (CTD)。

(3) 失效经验数据

失效经验数据用于向 GIDEP 会员告知非一致性部件、元器件、化学品、过程、材料、规范、试验仪器、安全, 以及包括健康危害在内的危险形势。这些数据还包括失效分析及由图书馆递交的问题描述、纠正措施等问题情报, 还有预防事故的经验教训报告。

主要包括以下 5 个方面的内容:

- 警报 (AL): 报告不符合规范的产品和程序的问题。这种非一致性在系统/设备中有很高的实效概率。
- 安全警报 (SA): 报告影响人和设备安全的问题。
- 问题顾问 (PA): 报告非一致性, 这种非一致性不同于 AL, 它发生功能失效的概率较低。报告不符合规范的产品问题和过程问题, 也可将其作为初始 AL, 由于缺乏数据支持还不能完全确认为 AL 的问题。
- 代理行为通告 (AN): 由政府代理处报告产品或过程的问题。不同于前几项, AN 不包含问题解决方法和制造商的纠正措施, 但是 AN 对发生的这些问题形成文件, 通告限制在一定范围内发布。
- 经验教训 (LL): 包括一些成功的工作实践, 也包括防止问题再次发生的教训和经验。

(4) 计量数据

计量数据包括试验和检查设备的校准程序、技术手册, 也包括关于校准图书馆、校准系统和测量系统的一些工程信息。国家标准和技术学院捐赠了一部分很有意义的关于测量科学的工程数据。

(5) 产品信息数据

制造商对元器件和材料特性进行更改的通告, 包含产品变更通知 (PCN), 产品信息通知 (PIN), PCN 主要报告如 MIL-STD-480 (已由 MIL-STD-973 替代) 定义的 1 类变更。制造商通过 PCN 来通知他们的客户关于影响产品形式、结构或可靠性的变更。一些典型的变更数据如下: 数据手册变更、工厂迁址、晶圆制造工艺、规范、芯片修改、运输标签、包装形式、器件标记、技术产权转让。

(6) 可靠性、维修性数据

可靠性、维修性数据包括与可靠性和维修性实践有关的理论、方法、技术和程序, 也包括失效率、失效模式、替代率数据 (都是基于设备、分系统、系统的现场性能和验证试验数据), 除了电子的 RM 数据, 数据库还包括了机械、机电、水力、气动力产品的 RM 信息。都说 GIDEP 的数据信息是和军用产品有关的, 事实

上 GIDEP 有商业产品的数据，已经把信息扩展到了 COTS 产品。

(7) 紧急数据请求 (UDR)

紧急数据请求是以 UDR 表的形式将会员的问题反馈给其他会员以获取帮助，迅速解决问题。

7.8.3 IHS

美国的 HIS 公司成立于 1959 年，是全球具有领先地位的关键信息、产品、解决方案和服务供应商，客户遍布全球 100 多个国家和地区，为六大核心行业中的政府机构与公司企业服务。致力于提供完备的信息解决方案，以提高客户效率、增强客户竞争优势，并在产品开发生命周期中的各个阶段为客户提供决策支持。其信息工具可以帮助用户快速、及时地获取大量相关信息和知识应用工具。订阅服务是公司的主要收入来源。IHS 公司拥有业内最全面的数据库，同时还采用了独有的流程与技术，能够有效收集、管理和交付大量的信息资源。

公司分为能源与工程两大运营部门，情况如下。

1. 能源部门

IHS 能源部门为石油和天然气行业提供全面的资讯服务，从油井、生产数据，到经济及咨询产品与服务无所不包。无论是评估有关地质、技术和开采潜力等底层问题，还是考虑各种政治、金融以及环境风险等可能造成的经济影响，IHS 能源部门的服务和解决方案均可为石油和天然气领域的专业人员提供必要支持。IHS 可为客户提供丰富信息，帮助客户快速做出明智决策，同时更好地控制和认识与石油、天然气勘探及开采相关的一系列风险。IHS 拥有 17 个技术团队，可提供 42 种语言的服务，业务范围覆盖全球 90 多个国家和地区的石油行业。

2. 工程部门

IHS 的工程部门为超过 100 个国家和地区的客户开发，并实施工程、技术以及监管信息解决方案。其解决方案包括通过定制解决方案提供的互联网订阅服务（如通过 IHS 企业解决方案提供的数据库转换、信息门户与系统集成服务）、CD 光盘和通过 IHS 全球工程文档提供的印刷文档。工程部门主要为以下行业提供解决方案：汽车、航空/航天、建筑、能源、政府/国防部门、电子/电信、石化以及公用事业。IHS 已获得 ISO 9001 认证。至今，IHS 的子公司和分销商遍布世界各地，构成了一个享有盛誉的销售与服务网络。

该公司在全球 22 个国家有超过 3500 名员工，其中 2007 年的市场份额为 38 亿美元，2007 年的收入有 6.884 亿美元。在 IHS 的客户中，35%来自美国财富 1000

强，60%来自全球财富 500 强。

客户可通过 IHS 订阅服务，实现快速通过互联网、DVD、企业内联网或外联网获得信息（通过选择所需的集合或选择所需行业，再输入需求的信息，单击“报价申请”可获取产品报价信息）。

IHS 提供的数据产品及服务包括：

- Parts Universe: 电子元器件数据库。
- IHS HAYSTACK Gold: 美军后勤管理数据库。
- CatalogXpress: 制造商目录数据库。
- BOM Manager: 管理复杂的产品物料构成，能自动监控和发出警报，能生产详细的报告。
- COMET: 关键元器件停产管理，可用预报和替代部件。
- PCNalert: 实用的供应商技术资料和需求信息呈现。
- BOM Optimizer: 物料清单优化。
- Parts Universe Materials Analysis: 环境适应性和寿命分析。
- EEEEC: 电子和电气设备符合性解决方案。
- CyberRegs: 调整的元器件库（Regulatory Compliance Library）等。

7.8.4 RIAC

美国可靠性信息分析中心（RIAC）是国防部特许的十个信息分析中心之一，主管单位为美国国防技术信息中心（DTIC），即美国国防部进行收集和分发科技信息的中心组织。

RIAC 成立于 1968 年，自 2005 年 6 月 21 日政府将一个新的 1,900 万美元的五年合同给了该中心，RIAC 也由原来的可靠性分析中心（RAC）更名为可靠性信息分析中心，名称的改变主要是为了强调 RIAC 是信息分析中心家族的一员。该中心在 2014 年已归属美国国防信息中心（DSIAC）。RIAC 目前已经形成了一个拥有数百人的团队，这个新的团队由表 7-29 所示的五个组织组成并共同运作。

表 7-29 负责 RIAC 运作的组织

承包商类别	部门	RIAC 职位	特长	网页地址	负责人
主承包商	Wyle 实验室	RIAC 主管	可靠性和环境试验服务	http://www.wylelabs.com/	Joseph Hazeltine
次承包商	Quanterion 公司	RIAC 技术主管	RIAC 大部分日常运营活动	http://quanterion.com/	Preston MacDiarmid

(续表)

承包商类别	部门	RIAC 职位	特长	网页地址	负责人
次承包商	马里兰大学 风险与可靠性 中心		R&M 教育, 系统和人因可靠性、元器件封装研究	http://www.enre.umd.edu/ http://www.calce.umd.edu/	Mohammed Modarres, PhD
次承包商	宾夕法尼亚 州立大学应用 研究实验室		机械可靠性、基于条件的维修 (CBM)、预测、总资产管理		Timothy Bair
次承包商	纽约州立大 学技术学院 (SUNYIT)		RIAC 挂靠处	(http://web.sunyit.edu/)	Heather Dussault, PhD

RIAC 是美国国防部唯一特许开展关于可靠性、维修性、质量、保障性和互操作性 (RMQSI) 方面信息工作的中心。在 RMQSI 方面提供咨询服务、指导出版发行, 以及按照 DTIC 管理的空军合同的要求对政府和工业部门进行培训。RIAC 在 SUNYIT 的实践是一个政府与学术界成功合作的典范, 实现了国防部门与工商业的技术互补。

自 1976 年, RIAC 开始培训工作的, 如今其培训项目已有 40 多门在线课程, 其已开展过可靠性相关学科的数千种技术与方法的培训。

RIAC 提供的可靠性数据资源在全世界享有盛誉。它拥有大量元器件/组件方面的定量和定性数据库, 并通过几种形式来提供这些数据。这些数据来源于众多的企业和政府试验与现场数据源, 并得到不断更新。下面是 RIAC 的数据产品:

- 电子部件可靠性数据手册 EPRD-97。
- 非电子部件可靠性数据手册 NPRD-95。
- 失效模式分布数据手册 FMD-2013。
- 静电放电敏感性数据手册 VZAP-95。

7.8.5 美国的核电可靠性数据系统 (NPRDS)

在 20 世纪 70 年代初期, 美国国家标准协会 (ANSI) 工业委员会和爱迪生电力协会 (EEI) 认识到核电站设备失效数据的重要性, 由此, 开发了一个数据收集系统, 目的是为与安全相关的系统和设备做一个可用的可靠性统计 (例如: 失效率、平均无故障时间和平均修复时间等)。这个核电站可靠性数据系统 (NPRDS) 由西南研究院 (SWRI) 开发完成。在 1974 年, 核电站开始自愿上报数据给 SWRI, 一直持续到 1982 年。1982 年 1 月, 美国核电运行研究所 (INPO) 开始管理这个系

统，一直到 1996 年底结束。NPRDS 最初的范围覆盖了按 ANSI 标准划分的安全一级、二级或 1E 级的系统和设备，只有少数设备除外，例如反应堆压力容器、堆内构件和乏燃料存储装置等。然而，后来范围被扩大，覆盖了任何一个安全重要系统，以及若丧失功能会引起电站严重瞬态的系统。到了 1984 年末，共有 86 个电站反应堆从 30 个系统中提供了 4000~5000 个设备的详细设计数据和失效报告。上报到 NPRDS 的数据有两类：工程报告和失效报告。对每一个需要报告的设备，工程报告提供了详细的设计和运行特性，失效报告提供了设备不能执行其既定功能的信息。NPRDS 提供给 INPO 的失效报告通常是业主利用维修记录类似维修工作申请形成的，这些报告使用了一套标准的设备边界和失效模式定义。

7.8.6 CEPREI_RDC

我国于 1980 年建立了“中国电子产品质量与可靠性信息交换网”，在工业和信息化部电子第五研究所设立了可靠性数据中心（CEPREI_RDC）。作为我国电子产品可靠性信息中心，该数据中心拥有海量元器件信息处理技术、手册编制、元器件分类、性能参数规范化、信息挖掘和信息定制技术，主要基础信息库包括如下内容。

1. 元器件基础信息库

元器件基础信息库包含元器件型号规格、制造商、质量等级、封装形式、主要性能参数、供货状态、执行标准、技术手册等信息内容。元器件基础信息库是元器件管理信息化的基础，是元器件标准化信息的来源，为产品研发、生产、维修保障提供信息基础。目前数据中心已建立的元器件基础信息库中包含约 500 万个型号规格元器件。

2. 元器件优选信息库

元器件优选信息库是在基础信息库的基础上，根据电子装备可靠性指标要求和使用环境特点，以及元器件的发展趋势、具体工程型号的元器件选用要求，遵循压缩品种、精选厂家的原则，对元器件进行等级划分所形成的，可有效指导元器件的优化选用，从而保证产品质量与可靠性。

3. 进口元器件停产信息库

数据中心收集了自 2000 年至今全球主要元器件生产商的元器件停产和功能修改通告，帮助企业及时掌握和应对元器件停产问题，避免设计选用停产器件，将因元器件停产带来的采购风险和造成的成本损耗降到最低。目前，数据中心已建立了 50 多万种进口元器件的停产信息库，信息项包含产品类别、名称、型号、制造商、

最后购买日期、停产日期、停产信息发布日期、发布来源等信息。

4. 元器件国产替代信息库

受国际军备竞争以及商业利益驱动的影响，当前，我国武器装备选用进口电子元器件面临着可能存在安全隐患、禁运受控、停产断档、假冒伪劣、质量等级无法满足装备使用要求等一系列问题。在此背景下，数据中心建立了元器件国产替代信息库，收集了进口器件对应的国产替代器件信息，并对替代器件之间的封装形式、质量等级、性能参数等进行了详细对比，为装备国产化提供了信息支撑。数据中心目前的国产化替代信息库中包含约 5 万个型号规格元器件。

5. EDA 软件原理符号库及封装符号库

为了提升电路设计水平，提高设计的规范性及标准化水平，提升设计效率，在设计工作中实现元器件的选用管理，建立了 Mentor、Cadence、Altium 三种主流 EDA 设计软件使用的原理图符号库及封装符号库，在设计软件中可直接调用，并以物资编码为关键字与元器件基础信息库保持信息同步，保证了设计 BOM 的信息准确性。目前已建立近 10 万种元器件型号规格的 EDA 图库。

6. 元器件可靠性预计参数库

为支撑可靠性预计工作，以 GJB/Z299C 和 MIL-HDBK-217F 等预计手册中各类别元器件的可靠性预计模型为基础，给出各类别元器件所需的各项可靠性预计参数，如集成电路的预计参数项包括：工艺、质量等级、门数/晶体管数、最大功耗、成熟度、电路类型、壳到结的热阻、管脚数、封装形式等详细信息，可帮助用户轻松实现可靠性预计。

7. 元器件降额参数库

为支撑降额设计工作，根据 GJB/Z 35 以及元器件分类的要求，不同类别的元器件降额参数栏目、各降额等级的降额程度都不相同，元器件降额参数库以元器件基础参数库为基础，结合 GJB/Z 35，给出了不同元器件类别、不同降额等级下的各种降额参数。

8. 元器件热仿真参数库

在产品的设计和可靠性仿真技术中，热设计和热仿真技术是一个非常重要的环节，通过建立元器件的热参数信息库，可以为产品的热设计和热仿真技术提供更加准确、完善的热性能参数，使得产品热设计和热仿真技术更为精确，大大减少热应力导致的失效问题，有效地器件材料参数等信息。

9. 元器件性能仿真模型库

现代高速数字系统设计需要进行信号传输线路的仿真分析,合理布局布线,作为仿真分析中必要的器件模型,Spice、IBIS 模型得到了广泛的应用。为了支撑信号完整性仿真等工作,建立了元器件性能仿真模型库。

10. 元器件机械振动仿真参数库

提供电子元器件详细的外形尺寸信息,并以此建立电子元器件通用的三维模型;结合主流力学仿真软件(Ansys, Adams 等)的材料参数库,建立电子元器件、焊接和 PCB 板通用材料的机械振动仿真参数库。实现模型和参数库的实时更新,以及与工具软件的无缝连接。

11. 元器件失效率水平信息库

为保证装备 RMS 各项工作的顺利开展,元器件的失效率水平的确定是至关重要的。在收集国外进口元器件制造进口元器件制造商公布的基于可靠性试验或现场统计的失效率水平数据,以及基于需方要求和主流可靠性预计手册的国内外元器件典型应用环境类别下的可靠性预计通用失效率数据,建立电子元器件失效率水平信息库。

12. 元器件三维模型库

当前电子设备复杂度、集成度越来越高,机械振动仿真和可制造性设计等工作的实施是势在必行,除了电子元器件的质量、材料等信息之外,最为基础的则为元器件的三维图形库。可以定制提供在各种机械振动分析和可制造性分析工具中使用的*.STEP 格式的通用元器件三维模型文件。

13. 元器件标准文献参考信息库

提供了国内外电子元器件的政策法规、标准规范、技术讲座、应用指南、技术动态、行业资讯等标准文献的参考信息。

参 考 文 献

- [1] IEC 60300-3-2:2004 Dependability management-Part3-2:Application guide—Collection of dependability data from the field.
- [2] GJB 1686-1993 武器装备质量与可靠性信息管理要求.
- [3] 工业和信息化部电子第五研究所数据中心. 可靠性数据的收集与处理. 可靠性工程系列讲义, 2003.



- [4] GB/T5080.6 设备可靠性试验 恒定失效率假设的有效性检验方法.
- [5] 赵宇. 可靠性数据分析. 北京: 国防工业出版社, 2011.
- [6] 贺国芳. 可靠性数据的收集与分析. 北京: 国防工业出版社, 1995.
- [7] 刘松, 等. 武器系统可靠性工程手册. 北京: 国防工业出版社, 1992.
- [8] 金星, 等. 可靠性数据计算及应用. 北京: 国防工业出版社, 2003.

第8章

可靠性评估

8.1 可靠性评估的作用

产品可靠性评估是指根据产品的可靠性结构、寿命分布模型，利用试验信息（或现场使用数据），运用统计学数值估计理论和方法，求得产品可靠性特征量的区间估计过程。典型的可靠性特征量为可靠度置信下限、MTBF 置信下限等。

产品可靠性评估的主要目的是：

- 定期评估电子装备达到的可靠性水平，并分析故障原因，提出纠正措施，实现产品的可靠性增长。
- 量化评估产品的可靠性水平，以确定产品的可靠性是否符合研制合同要求。

产品可靠性评估适用于研制和使用阶段的可靠性评价。

对于航天、航空、火工产品、大型复杂通信系统等复杂系统来说，受限于试验条件、试验费用及其他条件，开展可靠性试验进行产品的鉴定较为困难，另外，当前产品的可靠性较高，完全通过可靠性试验进行产品可靠性评价的费用也难以接受，因此，如何综合试验数据以及多源数据进行可靠性评估，成为当前可靠性分析评价中较为重要的一种方法。可靠性评估工作可在产品研制的任一阶段进行，尤其在产品定型时进行可靠性评估，是可靠性工作中不可缺少的环节，有着十分重要的意义。

可靠性评估工作的意义如下：

- 科学而先进的可靠性评估方法，为充分利用各种试验信息奠定了理论基础。这对减少试验经费，缩短研制周期，对合理安排试验项目、试验时间，协调系统中各单元的试验量等有重要的作用。
- 解决小子样产品、系统级可靠性试验难以开展的可靠性评估的重要工具，是有效解决航天器、火工产品、大型复杂通信系统等复杂系统可靠性评估的有效手段。



- 为系统的运筹使用提供条件，例如卫星发射机冗余数量的确定，需要给出单台发射机的可靠性、重量、经费等。
- 通过评估，检验产品是否达到了可靠性要求，并验证可靠性设计的合理性，如可靠性分配的合理性，冗余设计的合理性，选用元器件、原材料及加工工艺的合理性等。
- 评估工作会促进可靠性与环境工作的结合。在可靠性评估中，要定量地计算不同环境对可靠性的影响，要验证产品的抗环境设计的合理性，验证改善产品微环境的效果。
- 通过评估，可以指出产品的薄弱环节，为改进设计和制造工艺指明方向，从而加速产品研制的可靠性增长过程。
- 通过评估，了解有关元器件、原材料、整机乃至系统的可靠性水平，这为制订新产品的可靠性计划提供了依据。

8.2 可靠性评估的工作内容和程序

可靠性评估的主要工作内容和程序包括：确定并了解评估对象、任务分析、系统组成分析、试验计划分析、制订评估大纲、数据收集预处理、评估计算、结果分析与报告生成等，下面分别予以说明。

1. 评估工作的准备

制订可靠性评估大纲前，首先应确定评估对象并对其任务、综合试验计划 and 产品结构进行分析，以明确产品的组成、功能、使用环境和所能收集到的数据的质量和数量。

2. 任务分析

根据产品的任务阶段，确定各阶段的任务剖面，并对使用环境进行分析：

- 明确产品的功能及性能要求、故障定义，确定故障判据。
- 确定产品在任务阶段中所使用的环境应力水平和持续时间。
- 确定环境因子、评估模型和数据来源。
- 确定产品的任务时间和等效任务时间。任务时间应取最大值或典型值。

3. 系统组成分析

- 系统的分级和单元产品的划分。根据评估要求把产品系统逐级划分成分系统、设备、部件。这些组成系统的产品，应是有独立试验数据或有可靠性指标要求的产品。

- 在分析产品结构和功能的基础上建立可靠性逻辑树（见图 8-1）或可靠性框图。在图 8-1 中，长方形表示产品、分系统或设备，与门表示串联，或门表示并联，2/3 表示 3 中取 2 的表决系统。
- 确定评估的数学模型。
- 确定各层次产品合适的故障分布。故障分布可从大量的试验数据的工程分析中得出，也可从以往类似产品的试验数据的分析中得出。产品的故障数据一般服从指数或二项分布。在产品的故障分布未知的情况下，可以假设为指数、二项或其他分布；对于所有假设都应有工程经验或统计检验作为依据。

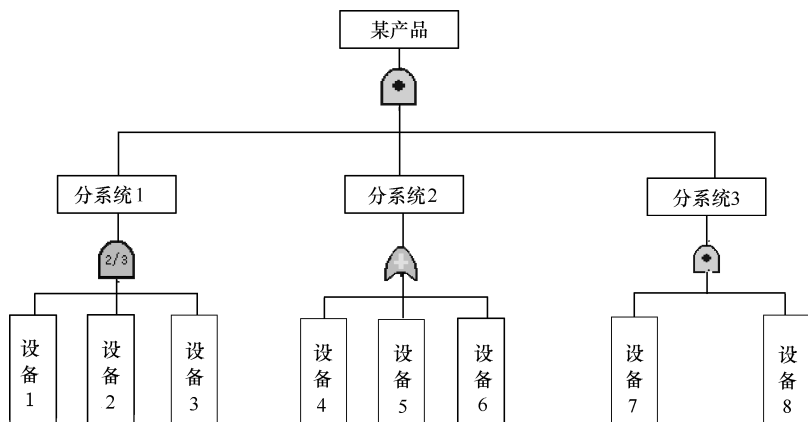


图 8-1 可靠性逻辑树示意图

4. 综合试验计划分析

在产品可靠性评估试验前，必须对综合试验计划进行分析。其主要目的是分析当前可利用的试验数据量以及需要补充开展的试验时间。通过综合试验计划的分析，最大限度地利用各种试验中所得到的数据，把专为可靠性评估而安排的试验压缩到最低限度。

- 明确各项试验的目的、持续时间及截尾方式。确定哪些试验的数据可用于可靠性评估，并确定收集数据的项目。
- 确定综合试验计划能否为可靠性评估提供充分的数据，如果不充分，应确定补充的试验项目。
- 对补充试验项目的截尾方式、试验时间和收集数据的项目提出相应的要求。

5. 制订可靠性评估大纲

根据产品的可靠性要求和技术要求，以及对产品的任务、结构和综合试验计划

进行分析，制订出可靠性评估大纲。大纲的主要内容包括：

- 评估组织机构。
- 规定评估的项目、内容及要求；制订可靠性评估的数据收集、处理、分析的程序及管理要求。详细给出各层次产品收集数据的范围、项目、精度，制订数据收集表格。
- 给出不同试验环境下的环境因子或其计算方法。
- 确定各层次产品的任务时间和等效任务时间。
- 确定各层次产品的失效分布。
- 给出故障判据。
- 给出区间估计的置信度。
- 按照产品特点和组成结构的差异，确定相应的评估模型。
- 确定分布检验、离群值检验的方法及显著性水平(α)。分布检验的 α 一般取 0.1，离群值检验的 α 一般取 0.01。
- 确定评估工作的进度安排。
- 确定评估报告格式。
- 可靠性评估大纲经评审批准后，成为产品可靠性评估的实施指引。

6. 可靠性评估数据的收集和处理

可靠性评估工作的有效性，在很大程度上取决于用于可靠性评估的数据收集的全面性、适用性分析以及数据处理的恰当性。例如：

- 若收集的试验数据不充分，评估得到的结果将不可信，关于判断试验数据是否充足的原则，可参阅相关资料。
- 若收集的试验数据不适用于可靠性评估而将这些数据用于可靠性评估，例如两个产品的设计，结构和原理都发生了较大的变化、更改，如果将其中一个产品的试验数据用于另一个产品的可靠性评估，所评估得到的结果也不可信。
- 收集到的试验数据，很多是在不同环境条件下开展的，需要将不同环境的试验数据折算到同一个环境条件下。例如，同一个型号的两个雷达设备 A、B，A 雷达设备的工作环境为 a（假设为地面良好，参考 GJB/Z 299C），B 雷达设备的工作环境为 b（假设为舰船普通舱内），当 A 雷达设备经过可靠性鉴定时，由于 B 雷达设备的工作环境与 A 雷达设备的工作环境不同，A 雷达设备的可靠性鉴定结果或可靠性评估结果，不能等同于 B 雷达设备，也就是说，B 雷达设备需要重新进行可靠性评估，评估时，可将 A 雷达设备的试验数据作为相似产品的试验数据，经过环境因子折算后，可用于 B 雷达设备的可靠性评估。

在开展可靠性评估数据收集工作时，制订相应的规程或操作规范，是非常有必要的。在规程或规范中，可从以下几个方面进行约束：

- 需要制订详细的数据收集、审核、归档计划和细则。
- 需要保证数据的完整性，制订相应的数据收集表格，完整记录产品数据、试验、使用数据，以及故障处理情况数据。
- 需要统一规定数据的来源、测量精度、计算方法、有效数字及其舍入规则。
- 需要保持数据的客观性，不得凭主观意志对数据任意取舍，不得凭猜测或推断填写数据。
- 数据收集表格必须在试验或现场使用的过程中及时准确地填写，不得事后补填。
- 数据收集表格的填写人员必须在表格上签名。
- 在数据的收集、汇总等环节应建立严格的审核制度，确保数据的真实性和准确性。
- 数据表格统一编号，防止丢失、遗漏或重复。
- 对数据进行归档或计算机储存。

7. 评估计算

根据评估大纲确定的评估方法及数学模型计算产品的可靠性特征量。一般可评估在计算得到不同置信度要求下，产品的平均故障间隔时间上下限、等效故障数。

在评估计算过程中，需要注意：

- 用于评估的数据，必须源于同一母体。不同环境的应力条件下的试验数据，需要经过试验数据适用性分析、环境因子折算后，才能用于评估。
- 可靠性评估计算，可计算单个设备的可靠性，也可采用金字塔式的评估方法，从组件、设备、分系统到系统，逐层进行可靠性评估。
- 可靠性评估一般可采用经典法、贝叶斯法等方法进行评估。可参阅相关资料，了解这些方法的使用方法。

8. 结果分析与报告编制

通过可靠性评估确定产品的可靠性是否达到规定的要求，并针对薄弱环节，分析原因，提出改进措施，以实现可靠性增长。

编写评估报告，主要包括：

- 产品的结构与任务分析。
- 确定的故障判据准则。
- 数据统计与分析。



- 可靠性评估模型与计算结果。
- 可靠性评估值与设计指标进行比较，分析装备的薄弱环节和提出改进设计的建议。

8.3 可靠性评估的数据收集和处理

8.3.1 可靠性评估数据的收集

可靠性评估数据的有效获取，实际上不仅仅是一个工程问题，更是一个管理问题。因此，最重要的就是要严密组织，加强管理，制定规章制度，以实现对信息的客观、科学的收集。对于可靠性评估数据的收集，最好能形成一个操作规范，在实践中工程技术人员要严格执行，以保证收集信息的完整性、可信性。

对于大型复杂系统的可靠性评估而言，获取可靠性评估数据的方式多种多样，可以概括为如下 6 种：

- 设备及分系统试验信息：由于系统的复杂性，一般采用金字塔式的可靠性评估方法，对设备和分系统进行大量的可靠性试验，以弥补系统级试验的不足，这里包括可靠性增长试验信息。设备及分系统在研制过程中的全部有关试验数据、故障信息及性能参数应当收集起来，以供可靠性评估。各分系统应向总体承制单位提供上述信息，将数据填入统计用表，以便评估。
- 仿真试验信息：可靠性仿真作为一门新兴的可靠性技术正在兴起，可靠性仿真试验信息可以为系统可靠性评估提供验前信息。同时，必须认识到，正确建立可靠性仿真模型和可靠性仿真模型的验证确认是可靠性仿真成败的关键，也是顺利完成仿真试验，得出可信结果的保证。
- 相似系统信息：相关型号的系统可以为可靠性评估提供验前信息，但是必须清楚相似系统与被评估系统之间的相互关系（结构、工作原理的区别，工作环境的区别），如果相似系统的结构、工作原理、工作环境都比被评估系统更苛刻，那么可以直接利用相似系统的信息，否则就需要进行信息的折算。
- 系统或单元在不同环境下的试验信息：为了考核系统的环境适应性或进行加速寿命试验，系统经常需要在不同环境下进行可靠性试验，试验要求各组成单元或系统的失效机理不变，运用此类信息需要研究利用环境因子进行折算。
- 专家意见及工程经验：在可靠性或安全性分析领域，专家意见或工程经验往往是十分重要的验前信息。
- 历史信息：包括单元或系统以往的各种试验信息。这是一类最可靠也是最可依赖的验前信息。问题的关键在于如何运用这些多环境、多试验阶段下的历史信息。

8.3.2 可靠性评估数据的处理

1. 失效分类处理

在复杂设备、系统可靠性评估中，应按照关联失效与非失效加以分类。只有关联失效的信息才用来估算可靠性参数。

(1) 关联失效

关联失效是指以下几种情况：

- 设备或部件因设计缺陷、工艺不良造成的失效。
- 设备中有数个元器件发生失效，但证明这些失效之间无从属关系。
- 设计寿命很有限的零部件，例如电池，其寿命在试验开始之前已经确定，在寿命期限終了之前出现的失效是关联失效。
- 任一设备出现间歇失效时，其首次失效应计为关联失效。
- 在老炼试验过程中发生的故障定为关联失效。

(2) 非关联失效

非关联失效是指以下几种情况，虽然它们不参与可靠性评估，但应记录在案。

- 因受试设备在试验箱内安装不当造成的失效。
- 因试验设备或监测仪器不良引发的失效。
- 因误操作引发的失效。
- 故障间的从属失效。
- 在检修故障过程中因检修不当发生的失效。
- 超过设计要求的过应力引发的失效。

(3) 关联失效转化为非关联失效

出现关联失效的设备经查明故障原因，采取改进措施，重新进行试验之后，确认改正措施有效时，可以将关联失效转化为非关联失效。

2. 验前信息的折算

相似系统试验信息和系统在不同环境下的试验信息必须经过相应的折算才能作为系统的验前信息来使用。验前信息的折算，一般包括以下两方面：

- 相似系统试验信息的折算。
- 不同环境试验信息的折算——环境因子的估计。

在实际利用环境因子进行不同环境信息的折算时，必须遵循以下 3 个前提条件：



- 条件 1: 失效机理一致性。在不同的应力水平下, 产品的失效机理保持不变。只有在失效机理保持一致性的情况下, 才能进行不同应力水平下可靠性信息的折算与综合, 环境因子的研究才有意义。通常情况下, 该假设可以通过试验设计来保证。
- 条件 2: 分布同族性。在不同的应力水平下, 产品的寿命服从同一形式的分布。该条件表明不同应力水平下的寿命数据的分布形式应相同, 只是在分布参数上存在差异。寿命分布同族性可以通过分布类型检验来保证。必须对子样的设计、制造状态进行定性分析或统计分析, 确定子样数据是否来自同一母体, 大多数情况下, 定性地分析子样是否根据相同的设计图样、相同的生产过程制造的, 就可以确认子样的一致性。如有怀疑, 可以采用经认可的统计方法进行分析。不是同一母体的子样数据不能一起进行可靠性评估。
- 条件 3: Nelson 假设。产品的残存寿命仅依赖于已累积的失效和当前应力, 而与累积方式无关。这一假设是由 Nelson 提出的, 它实际上是将累积失效概率作为环境对产品损伤作用的外在表现, 认为即使在不同环境下, 只要产品的累积失效概率相同, 产品中的累积损伤就是相同的。该假设具有明显的物理意义。

如需利用不同环境下的试验或使用数据进行可靠性评估, 则必须将不同环境下的试验或使用时间数据应用环境因子折算成基准环境下的等效试验或使用时间。

假定 B 为基准环境, A 是试验或使用环境, 当两种环境条件下的试验或使用数据较充分时, 可采用区间估计方法估算环境因子 K 。

假定 τ_A , τ_B 分别为环境 A 和环境 B 下的试验或使用时间, z_A , z_B 分别为环境 A 和环境 B 下试验或使用的关联故障数, 则有如下计算。

(1) 定数截尾

指数分布产品的环境因子为

$$K_L = \frac{\tau_B z_A}{\tau_A z_B} * F_{1-\gamma}(2z_A, 2z_B) \quad (8-1)$$

$$K_U = \frac{\tau_B z_A}{\tau_A z_B} * F_{\gamma}(2z_A, 2z_B) \quad (8-2)$$

在式 (8-1) 和式 (8-2) 中, K_L 为环境因子 K 的置信下限, K_U 为环境因子 K 的置信上限, γ 为置信度, $F_{\gamma}(2z_A, 2z_B)$ 是自由度为 $2z_A$ 、 $2z_B$ 的 F 分布的 γ 分位数 (参见 GB/T 4086.4)。

(2) 定时截尾

指数分布产品的环境因子为

$$K_L = \frac{\tau_B(2z_A + 1)}{\tau_A(2z_B + 1)} * F_{1-\gamma}(2z_A + 1, 2z_B + 1) \quad (8-3)$$

$$K_U = \frac{\tau_B(2z_A + 1)}{\tau_A(2z_B + 1)} * F_{\gamma}(2z_A + 1, 2z_B + 1) \quad (8-4)$$

当基准环境 B 比环境 A 较恶劣时, 环境因子 K 取 K_U , 反之取 K_L 。

当两种环境条件下的试验或使用数据不充分时, 可参考 GJB/Z 299C 给出的方法, 确定环境因子 K 。

对于产品的高温试验可用阿列尼兹 (Arrhenius) 公式折算环境因子。对于不同电压应力条件下的环境因子可通过逆幂律模型计算。

关于变母体、变环境等试验的环境因子折算方法, 可参阅相关资料。

3. 验前分布的检验

如前所述, 在可靠性评估时, 要保证分布同族性, 也就是说, 在可靠性评估中运用验前信息之前, 必须确定其分布类型, 以便选取对应的验前分布, 同时应用验前信息的前提是验前信息能够反映可靠性参数的统计特征, 即要求验前信息和现场试验信息近似服从统一总体, 这就需要对验前信息与现场信息进行相容性检验。

4. 子样数据的一致性检验

开展可靠性评估时, 需要确认用于可靠性评估的子样数据是否来自于同一母体。需要对子样的设计、制造状态进行定性分析或统计分析, 确定子样数据是否来自同一母体。在大多数情况下, 定性地分析子样是否根据相同的设计图样、相同的生产过程制造的, 就可以确认子样的一致性。如有怀疑, 可以采用经认可的统计方法进行分析。不是同一母体的子样数据不能一起进行可靠性评估。

5. 分布检验和离群值的检验

对子样数据应该进行分布检验, 以验证所假设的分布模型的适用性。当原假设被拒绝时, 应通过制图或统计方法、判断故障率是上升、恒定或下降, 以及子样数据的频率分布来选择其他适用的分布模型, 或进一步收集更多的数据进行分布模型确定。

关于分布检验方法, 指数分布可采用 GB/T 5080.6 给出的方法进行检验。为了提高数据的质量, 还应对数据进行离群值的检验, 对检出的离群值应分析其技术上或物理上的原因, 剔除确属离群的数据。对于离群值的检验方法, 指数分布可采用 GB/T 8056 给出的方法进行检验。

6. 变母体变环境的数据处理

在工程中, 为了在小数据样本的情况下评估产品的可靠性水平, 应扩大评估的信息量, 因此可以将产品在研制、使用中的各种可靠性数据进行综合评估, 目前的

变母体变环境的可靠性评估分为 3 种情况。

(1) 变母体数据的可靠性综合评估

常见的有杜安 Duane 模型、AMSAA 模型等。由于可靠性增长试验需要相当长的试验时间,而在我国可靠性研制费用普遍短缺,往往在工程上推行可靠性增长摸底试验,但由于试验时间偏短,进行可靠性评估的风险偏大,效果不甚理想。

(2) 变环境数据的可靠性综合评估

要利用产品在不同环境条件下的故障数据进行可靠性综合评估,关键的问题是要将不同环境条件下的试验结果转换为同一种环境条件下的试验结果。由于进行环境折合需要以大量的试验数据为基础,因此其实用性在工程上受到较大质疑。

(3) 利用相似产品信息的可靠性综合评估

通常可以采用贝叶斯方法,将相似产品信息作为先验信息引入到评估模型中。由于这种方法要求相似产品的数据与待评估产品的数据来自相同的试验环境,如果两者的试验环境有明显差异时,是无法进行综合的。

对于变母体的数据,例如,雷达在研制试验过程中发生了故障,经过故障分析并采取了相应有效的纠正措施,其可靠性会因此而得到增长,使得雷达的母体发生变化,因此,这种可靠性增长的特性可以用可靠性增长模型来描述。但是由于研制阶段的可靠性增长不同于单纯的可靠性增长试验,其各个试验的环境也不尽相同,所以,要处理这些数据,还应考虑不同环境的折合问题。

8.4 设备的可靠性评估方法

8.4.1 成败型设备的可靠性评估

设备的试验数据仅是成功与失败两种类型,记 $n=f+s$ 次试验,其中 s 为成功次数, f 为失败次数,则该设备的置信度为 γ 的可靠性置信下限 R_L 由下式确定:

$$\sum_{x=0}^f \binom{n}{x} R_L^{n-x} (1-R_L)^x = 1-\gamma \quad (8-5)$$

当 $f=n$ 时,上式无解,由正则性规定 $R_L = 0$ 。

当 $f=0$ 时:

$$R_L = (1-\gamma)^{1/n} \quad (8-6)$$

R_L 也可用下式直接计算:

$$R_L = \left(1 + \frac{f+1}{n+f} \times F_\gamma(2f+2, 2s) \right)^{-1} \quad (8-7)$$

式中, $F_\gamma(2f+2, 2s)$ 是 $F(2f+2, 2s)$ 分布的 γ 分位数。式 (8-7) 可查 GB 4089.3 求解。

8.4.2 指数寿命型数据可靠性评估

1. 定数截尾

(1) 无替换情形

有 n 个设备同时投入试验, 试验中出现失效设备不修复, 不替换, 事先规定试验进行到出现第 Z 个失效时终止。 Z 个数据按失效时间长短排序为:

$$t_{(1)} \leq t_{(2)} \leq \cdots \leq t_{(Z)}$$

得到总试验时间:

$$T_Z = \sum_{i=1}^Z t_{(i)} + (n-Z)t_{(Z)}$$

则设备置信度为 γ 的失效率置信上限:

$$\lambda_u = \chi_\gamma^2(2Z) / 2T_Z \quad (8-8)$$

设备置信度为 γ 的 MTBF 置信下限:

$$\theta_L = 2T_Z / \chi_\gamma^2(2Z) = \lambda_u^{-1} \quad (8-9)$$

设备置信度为 γ 的可靠性置信下限:

$$R_L = \exp\{-\chi_\gamma^2(2Z) / 2\eta\} \quad (8-10)$$

式中: $\chi_\gamma^2(2Z)$ ——自由度为 $2Z$ 的 χ^2 分布的 γ 分位数;

$\eta = T_Z / t_0$ ——等效任务数, 其中 t_0 为设备的任务时间。

(2) 有替换情况

试验方案与定数截尾无替换方案相同, 不同点仅是: 当设备出现失效时, 立即用同型号的新设备替换后接着试验, 使受试样本始终保持 n 个。获得的 Z 个数据按失效时间长短排列为:

$$t_{(1)} \leq t_{(2)} \leq \cdots \leq t_{(Z)}$$

待定数截尾有替换情形下的总试验时间:

$$T_Z = nt_{(Z)}$$

则设备置信度为 γ 的失效率置信上限:

$$\lambda_u = \chi_\gamma^2(2Z) / 2nt_Z \quad (8-11)$$

设备置信度为 γ 的 MTBF 置信下限:

$$\theta_L = 2nt_Z / \chi_\gamma^2(2Z) = \lambda_u^{-1} \quad (8-12)$$

设备置信度为 γ 的可靠性置信下限:

$$R_L = \exp\{-\chi_\gamma^2(2Z)/2\eta\} \quad (8-13)$$

式中, $\chi_\gamma^2(2Z)$ 、 η 的定义同式 (8-10)。

2. 定总试验时间

(1) 有替换情形

有 n 个设备投入 (可同时, 也可不同时) 试验, 一旦出现设备失效, 就用同型号的新设备替换, 试验直到各受试设备试验时间的累积总和达到事先规定的时间 T 为止。试验终止时发现 Z 个设备失效。累积总试验时间 $T_Z = T$, 则设备置信度为 γ 的失效率置信上限:

$$\lambda_u = \chi_\gamma^2(2Z+2)/2T \quad (8-14)$$

式中, $\chi_\gamma^2(2Z+2)$ 表示自由度为 $(2Z+2)$ 的 χ^2 分布的 γ 分位数。

设备置信度为 γ 的 MTBF 置信下限:

$$\theta_L = 2T / \chi_\gamma^2(2Z+2) = \lambda_u^{-1} \quad (8-15)$$

产品置信度为 γ 的可靠性置信下限:

$$R_L = \exp\{-\chi_\gamma^2(2Z+2)/2\eta\} \quad (8-16)$$

式中, T 为事先规定的值; $\eta = T/t_0$, t_0 和 $\chi_\gamma^2(2Z+2)$ 的定义同式 (8-14)。

(2) 无替换情形

有 n 个产品同时投入试验, 在试验过程中出现失效时可用同型号的新产品替换, 一直试验到各受试产品试验时间的累积总和达到事先规定的时间 T 为止。设此时间有 Z 个产品失效, 则产品置信度为 γ 的失效率置信上限同式 (8-14); 产品置信度为 γ 的 MTBF 的置信下限同式 (8-15); 产品置信度为 γ 的可靠性置信下限同式 (8-16)。

3. 定时截尾

(1) 有替换情形

n 个产品同时投入试验, 在试验过程中出现产品失效, 用同型号新品替换, 一直试验到事先规定的截尾时间 T 为止。设此时有 Z 个产品失效, 累积总试验时间 $T_Z = nT$, 则:

$$\lambda_u = \chi_\gamma^2(2Z+2)/2nT \quad (8-17)$$

产品置信度为 γ 的 MTBF 置信下限:

$$\theta_L = 2nT / \chi_\gamma^2(2Z+2) = \lambda_u^{-1} \quad (8-18)$$

产品置信度为 γ 的可靠性置信下限:

$$R_L = \exp\{-\chi_\gamma^2(2Z+2)/2\eta\} \quad (8-19)$$

式中, $\eta = \frac{nT}{t_0}$; t_0 表示任务时间; $\chi_\gamma^2(2Z+2)$ 的定义同式 (8-14)。

(2) 无替换情形

n 个产品同时投入试验, 在试验过程中出现产品失效, 不用同型号新产品替换一直试验到事先规定的截尾时间 T 为止。设 n 个产品的寿命分别为 t_1, t_2, \dots, t_n 。假设在事先规定的 T 时间内, 有 Z 个产品失效, Z 是随机变量。总试验时间为

$$T_Z = \sum_{i=1}^Z t_i + (n-Z)T$$

产品置信度为 γ 的失效率置信上限:

$$\lambda_u = \chi_\gamma^2(2Z+2)/2T_Z \quad (8-20)$$

产品置信度为 γ 的 MTBF 置信下限:

$$\theta_L = 2T_Z / \chi_\gamma^2(2Z+2) \quad (8-21)$$

产品置信度为 γ 的可靠性置信下限:

$$R_L = \exp\{-t_0 / Q_\gamma\} \quad (8-22)$$

式中, t_0 表示任务时间。

8.5 基于经典法的复杂系统可靠性评估

CMSR 法是修正极大似然法和逐次压缩法的综合、改进方法。它根据设备、分系统及系统的各级试验信息 (对于指数寿命分布单元应综合利用单元失效率预计数据), 估算复杂设备可能达到的可靠度。

8.5.1 成败型 (二项分布) 串联系统可靠性评估

m 个单元串联, 第 i 个单元的试验数据为 (s_i, n_i) , n_i 为单元 i 的试验次数, s_i 为

单元 i 的成功次数, 串联系统可靠度的点估计 \hat{R} 和方差 $D(\hat{R})$ 分别为:

$$\hat{R} = \prod_{i=1}^m s_i / n_i \quad (8-23)$$

$$D(\hat{R}) \approx \sum_{i=1}^m \left[\frac{\hat{R}}{\hat{R}_i} \right]^2 \frac{\hat{R}_i (1 - \hat{R}_i)}{n_i} \quad (8-24)$$

将 m 个单元串联, 综合结果等效于系统试验 n 次, 成功 s 次, 则:

$$\left. \begin{aligned} n &= \frac{\prod_{i=1}^m n_i / s_i - 1}{\sum_{i=1}^m 1/s_i - \sum_{i=1}^m 1/n_i} \\ s &= n \prod_{i=1}^m s_i / n_i \end{aligned} \right\} \quad (8-25)$$

式 (8-25) 统称为修正极大似然 (MML) 公式。

在给定置信度 γ 的情况下, 根据 n 、 s 、 γ 查 GB 4087.3, 即得 m 个单元串联系统的可靠性置信下限。

当存在 n_i 绝对最小且 $s_i = n_i$ 的单元 (即 m 个单元中试验次数最小的单元没有失效出现) 时, 不能直接运用式 (8-25), 应采用下面的 CMSR 方法进行评估。

设 m 个单元的试验中, 有 j 个无失效, 将 m 个单元按样本 (试验次数) 大小分别排序:

$$\begin{aligned} n_1 &\geq n_2 \geq \dots \geq n_{m-j} (n_i \neq s_i; i = 1, 2, \dots, m-j) \\ n_{m-j+1} &\geq n_{m-j+2} \geq \dots \geq n_m (n_i = s_i; i = m-j+1, m-j+2, \dots, m) \end{aligned}$$

之后 j 个无失效单元相当于一个单元进行了试验 (s_m, n_m) , 对 (s_i, n_i) , (s_m, n_m) 进行了一次压缩综合后得 (s'_{m-j}, n'_{m-j}) , 其中, 当 $s_{m-j} < n_m$:

$$\left. \begin{aligned} s'_{m-j} &= s_m \\ n'_{m-j} &= n_{m-j} n_m / s_{m-j} \\ s'_{m-j} &= s_{m-j} s_m / n_m \\ n'_{m-j} &= n_{m-j} \end{aligned} \right\} \quad (8-26)$$

这样根据数据 (s_1, n_1) , $(s_2, n_2) \dots (s_{m-j-j}, n_{m-j-j})$, (s'_{m-j-j}, n'_{m-j-j}) 可用式 (8-25) 计算 n 和 s 。在给定置信度 γ 的情况下, 根据 n 、 s 及置信度 γ 查 GB 4087.3 即得可靠性置信下限。

8.5.2 二项分布单元并联系统的可靠性评估

设 m 个成败型单元并联, 第 i 个单元的试验数据为 (s_i, n_i) 。若第 j 个单元失效, 则令 $s_j = n_j - 1$, 即假设该单元失效数为 1。

并联系统可靠性的极大似然估计和方差为:

$$\hat{R} = 1 - \prod_{i=1}^m (1 - \hat{R}_i) \quad (8-27)$$

$$D(\hat{R}) = \sum_{i=1}^m \left[\prod_{\substack{j=1 \\ j \neq i}}^m (1 - \hat{R}_j) \right]^2 D(\hat{R}_i) \quad (8-28)$$

式中, $\hat{R}_i = s_i / n_i$, 为单元 i 可靠性估计; $D(\hat{R}_i) = \hat{R}_i(1 - \hat{R}_i) / n_i$, 为方差。

系统等效试验数据为:

$$\left. \begin{aligned} n &= \frac{\prod_{i=1}^m \frac{n_i}{n_i - s_i} - 1}{\sum_{i=1}^m \frac{1}{n_i - s_i} - \sum_{i=1}^m \frac{1}{n_i}} \\ s &= n \left[1 - \prod_{i=1}^m \left(1 - \frac{s_i}{n_i} \right) \right] \end{aligned} \right\} \quad (8-29)$$

在给定置信度 γ 的情况下, 根据 s 、 n 、 γ 查 GB 4087.3, 可得并联系统的可靠性置信下限。

8.5.3 寿命型（指数分布）单元串联系统的可靠性评估

L 个指数分布单元串联系统可靠性的极大近似估计及方差为:

$$\hat{R} = \prod_{i=1}^L e^{-x_i / \eta_i} \quad (8-30)$$

$$D(\hat{R}) \approx \sum_{i=1}^L \bar{R}^2 Z_i / \eta_i^2 \quad (8-31)$$

式中: η_i ——第 i 个单元试验的等效任务数, 等于该单元试验时间 T_i 对该单元任务时间 t_i 之比;

z_i ——第 i 个单元试验的等效数, 对于定数截尾试验, z_i 等于实际失效数 r_i , 对非定数试验, 若 $r_i=0$, 则 $z_i=1$, 否则 $z_i=r_i$ 。

$$T_i = \sum_{j=1}^{n_i} t_{ji} + (n_i - r_i)t_{ri} \quad (8-32)$$

式中： t_{ji} ——单元 i 的第 j 个样本失效时的试验时间；

n_i ——单元 i 的试验样本总数；

t_{ri} ——定数截尾时，单元 i 的最后一个失效样本失效时的试验时间；当非定数截尾时，它为单元 i 的试验截止时间。

串联系统的等效试验数据为：

$$\left. \begin{aligned} \eta &= \frac{\sum_{i=1}^L z_i / \eta_i}{\sum_{i=1}^L z_i / \eta_i^2} \\ z &= \eta \sum_{i=1}^L z_i / \eta_i \end{aligned} \right\} \quad (8-33)$$

如果系统本身还有试验结果 (η_o, r_o) ，则先做 (η, z) 与 (η_o, r_o) 的相容性检验，相容时可综合数据为 $(\eta + \eta_o, z + r_o)$ 。若不相容则应认真分析、审查各单元及系统试验信息中的故障次数，时间收集的准确性与真实性，必要时应舍弃 (η, z) ，由 (η_o, z_o) 直接进行系统可靠性评估。置信度为 γ 的系统可靠性置信下限为：

$$R_L = \exp \left[-\frac{\chi_{1-\gamma}^2 (2r_o + 2z)}{2(\eta_o + \eta)} \right] \quad (8-34)$$

如果没有系统试验数据 (η_o, r_o) ，则按 (η, z) 进行评估。 χ^2 分布分位数可查 GB 4086.2。

为了增大评估的信息量，把各单元预计的失效率数据作为试验信息综合利用，此时单元 i 的数据 (η_i, z_i) 取为：

$$\left. \begin{aligned} \eta_i &= \eta'_i + 1/(\lambda_i t_i) \\ z_i &= z'_i + 1 \end{aligned} \right\} \quad (8-35)$$

式中： (η'_i, z'_i) ——单元 i 的试验数据；

λ_i ——单元 i 的预计失效率；

t_i ——单元 i 的任务时间。

同样要做 $(1/(\lambda_i t_i), 1)$ 与 (η'_i, z'_i) 的相容性检验。若相容，则可把式 (8-35) 代入式 (8-30) ~ 式 (8-33) 中计算；否则应认真分析，审查各单元失效信息、失效率数据的真实性与准确性，必要时应舍弃 $(1/(\lambda_i t_i), 1)$ ，只考虑试验信息。

相容性检验的方法为：设检验的显著性水平为 α ，欲判断 (η, z) 与 (η_o, z_o) 的相容性，如果 z/η 落在如下区间之内：

$$\left[\frac{\chi_{1-a/2}^2(2z_o)}{2\eta_o}, \frac{\chi_{a/2}^2(2z_o+2)}{2\eta_o} \right] \quad (8-36)$$

则可判断为 (η, z) 与 (η_o, z_o) 相容, 可以做数据综合, 否则为 (η, z) 与 (η_o, z_o) 不相容。一般取 α 为0.01~0.1。

8.5.4 指数分布单元并联系统的可靠性评估

l 个指数分布单元并联, 单元 i 的试验数据为 (η_i, z_i) , η_i 、 z_i 的定义与计算按第8.5.3节的方法进行。系统可靠性的极大似然估计及方差为:

$$\hat{R} = 1 - \prod_{i=1}^l (1 - \hat{R}_i) \quad (8-37)$$

$$D(\hat{R}) = \sum_{i=1}^l \left[\prod_{j=1}^l (1 - \hat{R}_j) \right]^2 D(\hat{R}_i) \quad (8-38)$$

$$\begin{aligned} \hat{R}_i &= \exp(-z_i / \eta_i) \\ D(\hat{R}_i) &= \hat{R}_i^2 z_i / \eta_i^2 \end{aligned} \quad (8-39)$$

系统等效试验数据为:

$$\eta = \frac{\left\{ \frac{1}{\prod_{i=1}^l [1 - \exp(-z_i / \eta_i)]} - 1 \right\}^2 \ln \left\{ 1 - \prod_{i=1}^l [1 - \exp(-z_i / \eta_i)] \right\}}{\sum_{i=1}^l [\exp(-z_i / \eta_i) / (1 - \exp(-z_i / \eta_i))]^2 z_i / \eta_i^2} \quad (8-40)$$

$$z = -\eta \ln \left\{ 1 - \prod_{i=1}^l [1 - \exp(-z_i / \eta_i)] \right\}$$

系统可靠性下限由式(8-34)确定。

8.6 基于 Bayes 的复杂系统可靠性评估

8.6.1 由指数寿命型单元组成的系统可靠度

首先估算设备可靠度, 在此基础上估算各种逻辑结构下的系统可靠度。



1. 元器件失效率 λ 向等效特征量 (β, α) 的转化

从元器件向设备做金字塔式的可靠性评估时，有必要将元器件的失效率 λ 转化为等效特征量 (β, α) 。参数 β 代表元器件的累计运行小时数， α 代表该时段内元器件累计失效次数。

元器件失效率的置信限估算常以两种形式出现：

- 取双侧置信区 (λ_L, λ_U) ，其置信度一般取值 0.60 或 0.90。
- 以单侧置信上限 λ_U 的形式给出，其置信度通常取值为 0.60。

下面说明将 λ_U 转化为等效特征量 (β, α) 的近似处理方法。

设某个品种的元器件经计数法或应力分析法预计得到失效率置信上限 $\lambda_U(\text{fit})$ 值，由工程上常用的定时截尾试验方式下的失效率置信上限计算公式，并且考虑到非零次失效在统计数据处理上的方便，当选定 $\alpha=1$ 之后，可有：

$$\beta = 2.02232 / \lambda_U \times 10^9 \quad (8-41)$$

该 (β, α) 就是相对于给定单侧置信上限 λ_U 的元器件可靠性等效特征量，它将作为该品种元器件可靠性的验前信息。

2. 设备可靠性预计

假定单元设备由 N 个主要元器件相互独立地串联组成（允许其中含有部分相同的元器件）。每个元器件的失效率为 λ_j 。由式（8-41）给出相应的等效重量 (β_j, α_j) 。按下式计算设备可靠性的验前信息 (τ_0, z_0) ：

$$\left. \begin{aligned} \tau_0 &= \sum_{j=1}^N \frac{\alpha_j}{\beta_j} \bigg/ \sum_{j=1}^N \frac{\alpha_j}{\beta_j^2} \\ z_0 &= \tau \sum_{j=1}^N \frac{\alpha_j}{\beta_j} \end{aligned} \right\} \quad (8-42)$$

式中： τ_0 ——设备折合运行小时数（h）；

z_0 ——设备折合失效次数；

α_j ——第 j 个元器件的折合失效次数；

β_j ——第 j 个元器件的折合试验小时数（h）。

信息 (τ_0, z_0) 表达了该设备可靠性的验前特征量。据此可用下式预计设备已初步具备的失效率置信上限 A_0 和可靠度置信下限 R_{L0} 。

$$\left. \begin{aligned} A_0 &= \chi_{1-\gamma}^2(2z_0) / 2\tau_0 \\ R_{L0} &= \exp(-A_0 t) \end{aligned} \right\} \quad (8-43)$$

式中: t ——设备任务时间 (h);

γ ——给定置信度;

$\chi^2_{1-\gamma}(2z_0)$ ——自由度为 $2z_0$ 的卡方分布置信单边上侧分位数;

A_0 ——可由 GB 4086.2 求得, 也可由软件算出。

设备的折合平均无故障寿命时间的置信下限为:

$$\theta_L = A_0^{-1} \quad (8-44)$$

3. 设备可靠性评估

上述的设备可靠性预计引入了置信度概念, 目的是将可靠性预计与可靠性评估从方法论上统一起来, 视预计为评估的特例, 以便将可靠性预计所得信息转化为复杂设备可靠性评估的验前信息加以利用。

假定设备经过一系列筛选和考核试验, 累计收集到现场试验信息 (τ_1, z_1) 。联合设备的验前信息 (τ_0, z_0) , 在共轭分布假定下经贝叶斯推断, 可给出设备的可靠性验后特征量:

$$\left. \begin{aligned} \tau &= \tau_0 + \tau_1 \\ z &= z_0 + z_1 \end{aligned} \right\} \quad (8-45)$$

设备的失效率上限 A 和可靠度贝叶斯下限 R_L 分别为:

$$\left. \begin{aligned} A &= \chi^2_{1-\gamma}(2z)/2\tau \\ R_L &= \exp(-At) \end{aligned} \right\} \quad (8-46)$$

4. 两类信息间的相容性检验

计算 (τ, z) 时, 应注意设备的验前信息 (τ_0, z_0) 与现场试验信息 (τ_1, z_1) 之间的统计相容性问题。这可借助于以下双边区间估计值进行统计显著性检验:

$$\left[\chi^2_{\frac{\alpha}{2}}(2z_1 + 1) / (2\tau_1), \chi^2_{1-\frac{\alpha}{2}}(2z_1 + 1) / (2\tau_1^2) \right] \quad (8-47)$$

α 称为显著性水平或风险, 取值 $0.01 \sim 0.1$ 。若验前信息的比值 z_0/τ_0 , 不为该区间所包含, 则拒绝两者的相容性假设。此时用式 (8-45) 计算 (τ, z) 视为无效, 这时需要核实原始信息的有效性, 尤其需要确认失效次数 z_1 , 是否有充分依据。当确认二者不相容时, 应当舍弃验前信息和放弃贝叶斯统计推断, 只用设备的现场试验信息 (τ_1, z_1) 进行经典意义下的设备可靠性评估。

8.6.2 串联系统可靠度

假设系统由 N 个相互独立的设备串联组成。当第 j 个设备的失效率服从伽玛密

度函数 $\Gamma(z_j, \tau_j)$ 时, 设备可靠性验后密度将是负对数伽玛函数。

对串联系统的概率密度函数用指数寿命分布下的一、二阶矩拟合, 可给出串联系统可靠度 R 的一、二阶矩:

$$\left. \begin{aligned} E(R) &= \prod_{j=1}^N \left(\frac{\eta_j}{\eta_j + 1} \right)^{z_j} \\ E(R^2) &= \prod_{j=1}^N \left(\frac{\eta_j}{\eta_j + 2} \right)^{z_j} \end{aligned} \right\} \quad (8-48)$$

式中: η_j ——第 j 个设备的等效任务数, $\eta_j = \tau_j / t_j$ 。

t_j ——第 j 个设备的任务时间。

(z_j, τ_j) ——第 j 个设备的验后特征量, 可由式 (8-45) 求得。

为了简化公式, 记一阶矩为 μ , 记二阶矩为 ν , 系统可靠性的特征量 (η, z) 由式 (8-49) 迭代解出:

$$\frac{\ln \left(\frac{\eta + 1}{\eta} \right)}{\ln \left(\frac{\eta + 2}{\eta + 1} \right)} = \frac{\ln \mu}{\ln \left(\frac{\nu}{\mu} \right)} \quad (8-49)$$

然后由下式解得串联系统可靠度贝叶斯下限近似解:

$$R_L = \exp \left[-\chi_{1-\gamma}^2(2z) / (2\eta) \right] \quad (8-50)$$

8.6.3 并联系统可靠度

假设系统由 N 个相互独立的设备并联组成, 该系统的可靠度函数为:

$$R = 1 - \prod_{j=1}^N (1 - R_j) \quad (8-51)$$

一般并联系统可靠度的贝叶斯下限之解难以获得, 为了工程应用, 只给出它的矩法近似解。当并联各设备都一样时, 可获得 R_L 的精确解, 即使采用矩法近似, 也可得到较高精度的近似解。

1. 一般并联系统的可靠度

第 j 个设备之 R_j 的验后密度为负对数伽玛函数, 对该并联系统进行梅林变换, 由卷积定理得系统不可靠度 $Q = (1 - R)$ 的验后密度之第 k 阶矩:

$$R(Q^k) = \prod_{j=1}^k \left[\sum_{i=0}^k (-1)^i C_i^k E(R_j^i) \right] \quad (8-52)$$

分别取 $k=1, 2$, 得:

$$\begin{aligned} E(Q) &= \prod \left[1 - \left(\frac{\eta_j}{\eta_j + 1} \right)^{z_j} \right] \\ E(Q^2) &= \prod \left[1 - 2 \left(\frac{\eta_j}{\eta_j + 1} \right)^{z_j} + \left(\frac{\eta_j}{\eta_j + 2} \right)^{z_j} \right] \end{aligned} \quad (8-53)$$

记 $E(Q)$ 为 ε , $E(Q^2) = \delta$, 从而有:

$$\begin{cases} E(R|\eta, z) = 1 - \varepsilon \\ E(R^2|\eta, z) = 1 - 2\varepsilon + \delta \end{cases} \quad (8-54)$$

记一阶矩为 μ , 记二阶矩为 ν , 表明尽管系统可靠度的确切验后密度未知, 但其一、二阶矩是可知的。将式 (8-54) 分别代入式 (8-49)、式 (8-50), 得到并联系统可靠度贝叶斯下限 R_L 近似解。

指数分布的并联结果不再是指数分布形式, 强行用负对数伽玛函数拟合未知并联系统的可靠度密度函数, 当受并单元可靠度低时, 计算结果将有可能产生较大的误差。

2. 相同设备并联时系统可靠性的精确解

在实际工程中, 为了提高系统可靠度, 常常使用一个或两个相同的设备做热备份。该系统可直接给出 R_L 的精确解。

假设系统由 N 个相同的指数寿命型设备并联而成, 每个设备的验后特征量为 (η_0, z_0) , 设备可靠度为 R_0 , 则系统可靠度的贝叶斯下限为:

$$R_L = 1 - \left\{ 1 - \exp \left[\frac{-\chi_{1-\gamma}^2(2z_0)}{2\eta_0} \right] \right\}^N \quad (8-55)$$

利用上式, 自然还可以进行并联系统的可靠性设计, 即给定 γ 、 R_L 条件下确定备份设备个数。

3. 相同设备并联下系统 R_L 的矩法近似解

当相同设备并联构成一个子系统时, 为了逐级综合评估系统可靠性, 更加关心的是给出该子系统的一、二阶原点矩。假设每个设备的可靠度为 R_0 , 其特征量为 (η_0, z_0) , 系统可靠性函数为:

$$R = 1 - \sum (-1)^i C_i^N R_0^i$$



则有以下近似解结果：

$$\left. \begin{aligned} \mu &= 1 - A \\ \nu &= 1 - 2A + B \end{aligned} \right\} \quad (8-56)$$

$$A = \sum_{i=0}^N (-1)^i C_i^N \left(\frac{\eta_0}{\eta_0 + i} \right)^{z_0};$$

$$B = \sum_{i=0}^{zN} (-1)^i C_i^{zN} \left(\frac{\eta_0}{\eta_0 + i} \right)^{z_0}$$

将公式 (8-56) 给出的 μ 、 ν 值代入式 (8-49)、式 (8-50)，即得特殊并联系系统可靠度的特征量及 R_L 的近似解。

8.7 可靠性评估案例

【例 8-1】 某电子装备试样在研制阶段进行无替换试验，共累积通电工作 786h，发现一次失效故障，试估计置信度为 0.7 时的 MTBF 置信下限。

解：通常，产品按试样研制计划进行试验，主管设计师认为产品性能已满足要求就停止试验，往往事先没有规定截止时间，我们把这种情况近似为定总试验时间截尾。

已知， $T=786$ h， $Z=1$ ，由式 (8-15) 得：

$$\theta_L = \frac{2T_Z}{\chi_{\gamma}^2(2Z+2)} = \frac{2 \times 786}{\chi_{0.7}^2(4)} = \frac{1572}{4.878} = 322.26\text{h}$$

即该电子装备在置信度为 0.7 时的 MTBF 置信下限为 322.26 h。

8.8 可靠性评估注意事项

开展可靠性评估工作时，需要注意以下事项：

- 无论是采用经典法、贝叶斯法还是其他评估方法进行可靠性评估时，需要确认所评估产品的技术状态是否稳定、固化。
- 在可靠性评估过程中，若使用产品研制过程中的数据以及相似产品的试验数据，例如可靠性预计数据，需要进行验前信息的相容性检验，若不相容，则以所评估对象的试验数据为准，进行可靠性评估。
- 可靠性评估工作，要基于一定量的试验数据进行。因此，在开展可靠性评估

工作时, 需要一定量的试验数据作为支撑。若完全没有试验数据, 则需要补充一定的试验数据再考虑采用可靠性评估方法进行产品可靠性评估。

- 应按复杂设备的工作时间和任务剖面, 分段评估其可靠性。对复杂设备的特殊功能及要求, 需要进行单项可靠性评估。

参 考 文 献

- [1] 周源泉. 可靠性评定. 北京: 科学出版社, 1990.
- [2] 刘松. 武器系统可靠性工程手册. 北京: 国防工业出版社, 1990.
- [3] 刘晗. 基于 Bayes 理论的小子样可靠性评定方法研究. 国防科学技术大学硕士学位论文, 2006.
- [4] 周广涛. 计算机辅助可靠性工程. 北京: 宇航出版社, 1990.
- [5] GB/T 3187. 可靠性基本名词术语及定义.
- [6] GB/T 4086.1~4086.6 统计分布数值表.
- [7] GB/T 4087. 数据的统计处理和解释. 二项分布可靠度置信下限.
- [8] GB/T 5080.6. 设备可靠性试验. 恒定失效率假设的有效性检验.
- [9] GB/T 8056. 数据的统计处理和解释. 指数样本异常值判断和处理.
- [10] GJB/Z 299C. 电子设备可靠性预计手册.
- [11] GJB 376. 火工品可靠性评估方法.

第9章

软件可靠性

9.1 引言

在装备系统中，无论是硬件，还是软件，只要发生故障都会使系统的完好率降低。例如，对于军事指挥员来说，他所关心的是使系统具有最高的战备完好率。为了向指挥员提供一个战备完好率满足要求的系统，软件可靠性和硬件可靠性同等重要。

硬件可靠性作为一门学科，最早用于第二次世界大战期间估算弹道火箭发射成功的概率。在过去的 70 多年里，硬件领域已建立了一套定量规定、预计和测定设备与系统可靠性的实用程序，并得到了公认。这些程序在许多规范、标准及手册中已有详细介绍。相对而言，软件可靠性是一门较年轻的学科，是软件工程和可靠性工程相结合产生的前沿技术。20 世纪 70~80 年代是软件可靠性的初创时期；20 世纪 90 年代是软件可靠性从纯粹的理论研究向工程应用的过渡时期；20 世纪末，新技术、新范例、新的结构分析概念以及新手段在软件开发领域蓬勃发展，软件可靠性也得到了快速地发展；21 世纪，随着互联网时代的到来，云计算、大数据等新兴产业极大地推动了软件技术的进步，人们对软件可靠性的需求也与日俱增。

然而，在软件可靠性的研究中仍然存在诸多问题。主要表现在：

- 其定义尚有分歧。
- 尚无工程认可的定量方法可供使用。
- 已提出相当多的可靠性预计模型，但似乎没有一种模型的有效性已经过充分的验证。
- 尚无可用的验证程序。

因此，开展软件可靠性的研究，提高软件的质量，进而提高系统的可靠性和完

好率具有重要意义。

9.2 基本定义和术语

9.2.1 软件的定义

对软件的定义有各式各样的版本，代表性的有：

① 在我国国家标准 GB/T 11 457-2006《信息技术软件工程术语》和国家军用标准 GJB 2786A-2009《军用软件开发通用要求》中的定义是：与计算机系统的操作有关的计算机程序、规程可能相关的文档。

② 在 NASA-GB-1704.13-96《安全关键软件的分析 and 开发指南》中的定义是：计算机程序和计算机数据库；有组织的能够控制设备运行的信息集。

9.2.2 软件可靠性的相关术语

软件可靠性涉及以下几个基本术语。

- 故障 (Fault)：任何被看成异常并可能有理由要求进行某种纠正措施的产品状态的变化。在一些文章中对软件故障的通俗解释是：软件故障是那些可能引起软件失效的状态。
- 差错 (Error)：工程需求、规格说明或设计中的错误，可能引起失效的设计、实现或运行中的错误。在一些文章中对软件差错的通俗解释是：软件差错是指那些软件实现与理论要求之间的差异。这个词在不同标准中有不同的定义和解释。
- 失效 (Failure)：系统或部件不能在规定的性能要求范围内执行其要求的功能。在一些文章中对软件失效的通俗解释是：软件运行中的异常行为。
- 缺陷 (Defect)：该词没有确定的解释。在一些文章中认为软件缺陷一词只是软件故障或软件失效的一般性叫法，具体含义依赖于它被使用的环境。

关于这些术语之间的关系说法不一，其中，IEEE 标准的解析应用较广，其对差错、故障和失效之间关系的解释为：差错—故障—失效，即由软件差错引发软件故障，导致软件失效。事实上这些术语的严格定义是件很困难的事，但其大概的内涵并非难于理解，基于以上 IEEE 的解析，我们可以得到这些术语之间的因果关系，如图 9-1 所示。

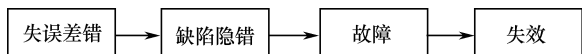


图 9-1 软件可靠性基本术语之间的因果关系



通常，软件可靠性的度量是对软件系统在规定的环境内，指定输入范围时无故障工作的概率的描述，因此，将软件可靠性定义为“在规定时间内，规定的条件下，软件不引起系统失效的概率”，这个概率是输入和系统利用的函数，也是潜在的软件故障发生的函数。系统的输入决定了在系统工作期间是否会遇到潜在的故障。

9.3 软件故障的分类

将软件故障分类便于分析和研究故障的原因与机理、现象与规律、后果与对策，如仿真软件的某种失效，有可能是需求阶段的物理模型有问题，也可能是设计阶段仿真算法与物理模型的逼近有问题（收敛性问题），还可能是设计阶段仿真算法在计算机上的舍入误差控制有问题（数值稳定性问题），以及实现阶段的代码编程有问题。软件错误的出现在一定程度上取决于软件分析师、设计师、程序师的知识水平。软件故障有多种分类方法，按软件故障产生特征、故障起源、故障后果可以对软件的故障分类如下。

1. 按故障产生特征分类

- 偶然故障：非故意造成的缺陷或隐错所形成的故障。
- 有意故障：故意造成的缺陷或隐错所形成的故障，大多是恶意的。

2. 按故障起源分类

（1）按故障起源的空间范围分类

- 内部故障：软件内部固有的缺陷或隐错所形成的故障。
- 外部故障：软件的外部环境造成的异常情况所形成的故障。

（2）按故障起源的发生时间分类

- 设计故障：软件开发和维护过程中形成的故障。
- 运行故障：软件运行过程中产生的故障。

（3）按故障发生的根本原因分类

- 因知识水平不到位而无法避免的错误：例如某些复杂的动力学控制系统（导弹飞行控制系统等），其计算机的舍入误差造成的影响尚无完善的理论分析，因此我们选择的算法可能在某些条件下存在缺陷，这是难免的。
- 因知识水平已到位但技术条件不到位而无法避免的错误：例如对复杂的异常处理（计算结果的实时运算溢出等），在汇编语言甚至 FORTRAN、C 等高级语言中都没有提供用于纠正实时运行错误陷阱的功能，使编写出的软件可

能在异常处理方面存在某种缺陷，这也是难免的。

- 知识水平已到位且技术条件已到位但不该出现的错误：例如我们将公式 $C=A+B$ 写成 $C=A-B$ ，这是无论如何不该出现的错误。又如 Visual Basic 和 ADA 语言已经提供了错误陷阱的功能来规避实时运行的故障，而我们没有利用此功能解决需求中规定的计算溢出处理的要求，这属于不该出现的错误。

3. 按故障后果分类

(1) 按故障后果的风险大小分类

- 安全关键故障：其后果可能给系统带来不可接受的风险的故障。
- 非安全关键故障：其后果不给系统带来不可接受的风险的故障。

(2) 按故障后果的影响类型分类

- 安全性故障：影响系统安全性服务的故障。
- 任务关键故障：影响系统完成规定任务的故障。

在上述定义中，安全关键故障必为安全性故障，任务关键故障可能为安全关键故障。虽然这种分类似乎还有不尽如人意之处，但这仍不失为一种有益的具有参考价值的分类。

当前最重要的、首先要解决的问题是，通过一系列的规范、标准、准则、指南、约定等约束，来有效地防范、减少、避免那些知识水平和技术条件均已到位但因不该出现的软件错误而导致的故障。

9.4 软件可靠性与硬件可靠性

9.4.1 软件可靠性与硬件可靠性之间的区别

软件可靠性与硬件可靠性存在很多不同之处，主要的差别有：

① 软件的寿命与它的失效率无关。如果软件过去可以运行，其他各项保持不变（即硬件、软件或接口无改变），将来也可以运行，软件没有生锈或用坏等硬件的机理损耗。

② 软件应用的频度不影响软件可靠性。同一个软件可以重复使用，并且如果第一次使用时不失败，以后任何一次同样的使用（硬件、软件或接口无改变，输入范围不变）也不会失败。与之相反，用旧的物理元器件会导致失效。

③ 当用户界面标准更改且硬件被废弃不用时，软件也没用了。

- ④ 除了记录、保存或转换用的媒体外，软件不像硬件那样可以触摸到。判断硬件产品的典型手段包括观察尺寸、分析组成成分、查看装配质量（形状、装配和涂层），以及分析使用是否符合技术规范。例如，可观察两个齿轮的啮合程度，或晶体管是否达到电路要求的电流量，这些物理概念均不适用于软件。
- ⑤ 不能用硬件的方法在使用前判断软件，例如没有等效的进货检查。
- ⑥ 软件能被测试前，软件必须和硬件匹配。如果发现失效，问题可能出在硬件、软件或硬件/软件接口的某个未曾预料的交互作用中。
- ⑦ 通常硬件可以在或不在一个给定的应用环境中工作，除非全部失效，软件按照其复杂性和功能性有不同的成功等级。
- ⑧ 尽管不可执行，技术文件通常被认为是软件的一部分。未能全面地或准确地描述运行过程中技术文件，被认为是像软件崩溃一样重大的失效。当一位用户期望得到在线帮助而没有得到时（或者因为没有被激活，或者因为提供的文件不完整或不正确），软件未满足用户的要求，因此不是非常可靠。相反，在评价硬件可靠性时通常不涉及技术文件。
- 两者的区别整理如表 9-1 所示。

表 9-1 软件可靠性与硬件可靠性之间的区别

软 件	硬 件
故障主要是由于设计错误造成的，生产（复制）、使用及维修（不包括改正）的影响可忽略不计	故障可能是由于设计缺陷、生产、使用及维修造成的
不存在耗损现象，软件故障发生时没有征兆	故障可能是由于耗损或其他与能量相关的现象造成的，有时候在故障发生之前可能有征兆
可靠性与这些因素无关。随着时间的推移，可靠性可能得到提高，但这与工作时间无关，而是与检测并改正错误所做的努力有关	可靠性可能与老化或耗损有关，即故障率可能随着工作时间的增长而降低、不变或提高
不可修理。唯一的解决方法是再设计（再编程），如果在再设计后把错误去掉而没有引起别的错误，将获得更高的可靠性	可进行修理，经修理后设备可能更可靠
可靠性与时间无关。当执行一步错误的程序，或者错误的通道时发生故障	可靠性与时间有关，故障发生与工作（或储存）时间有关
外部环境不影响可靠性，但它可能影响程序的输入	可靠性与环境因素有关
可靠性不能根据任何的物理要素进行预计，因为它完全取决于设计中的人为因素，已提出某些先验方法	从理论上讲，可靠性可根据对设计及使用因子的了解来预计
如果并行的程序通道是相同的话，采用余度不可能提高可靠性。因为，如果一个通道发生故障，那么另外的通道会具有同样的错误。如果采用并行通道，每个通道具有不同的小组来编写和校验的程序，则有可能提供余度	采用余度往往可提高可靠性

(续表)

软 件	硬 件
故障通常不可能根据独立语句的分析加以预计。错误可能随机地存在于整个程序中，而且任何一个语句都可能出错。可靠性关键清单及 Pareto 故障分析不适用	故障可能以某种模式在系统的某些部件中发生，在某种程度上，可根据在这些部件上所加的应力及其他因素来预计这些故障模式，可靠性关键清单及故障的 Pareto 分析是很有用的技术
软件的接口是概念性的，不是可见的	硬件接口是可见的，即人们可看到一个 10 插脚的连接器
软件中尽管有标准化的逻辑结构，但没有标准零件	硬件采用标准部件作为基本的积木式组件

9.4.2 软件可靠性与硬件可靠性之间的相似之处

软件可靠性与硬件可靠性同时也存在相似之处，包括：

- 硬件可靠性是设备复杂度的函数，直观地看，软件可靠性也是复杂性的函数。
- 固态电子器件（如晶体管或微电路）制造得好，在长时间内观察可以发现没有耗损机理；造成失效的缺陷（不包括明显误用器件造成的失效）是在开始制造器件的过程中引入的，软件也是如此。
- 可利用可靠性增长试验来提高硬件可靠性，也就是利用试验-分析-纠正大纲来发现、确定及改正可能造成设备早期失效的失效模式及机理。这与在软件程序中寻找和消除“程序错误”并且据此提高其可靠性的做法相类似。

因此，研究成功的硬件方法与刚兴起的软件方法之间存在的双重性是有意义的，一旦这种双重性被接受，全部问题将可能简化，因为就整个系统而言，硬件及软件问题可能一起得到解决。

9.5

软件可靠性统计模型

建立软件可靠性模型旨在根据软件可靠性的相关测试数据，运用统计方法得出软件可靠性的预测值或估计值。

9.5.1 主要统计模型

故障数和故障率是最通用的故障统计参数，基于这两类统计参数，有以下 4 类统计模型：基于指数分布的统计模型、基于威布尔分布的统计模型、基于贝叶斯方法的统计模型、基于测试覆盖率的统计模型和利用跟随法的统计模型。

1. 基于指数分布的统计模型

指数模型通常假定软件处于运行状态，所有的故障相互独立，从单个独立故障到失效的时间 t 服从指数分布：

$$f(t) = \lambda \exp(-\lambda t)$$
(9-1)

可靠度计算公式为：

$$R(t) = \exp(-\lambda t)$$
(9-2)

到下一个失效的平均时间（MTTF）为：

$$MTTF = 1/\lambda$$
(9-3)

指数分布模型的一般情况如图 9-2 所示。

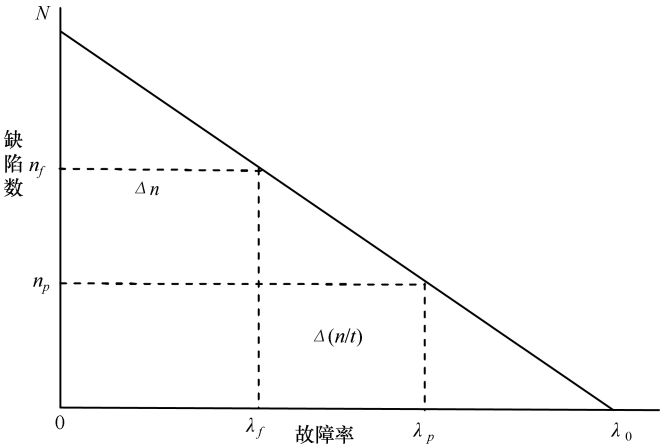


图 9-2 指数模型的基本要素

模型中的符号及参数说明如表 9-2 所示。

表 9-2 模型参数及说明

参 数	说 明	参 数	说 明
N	缺陷的总数	λ_i	故障率
n	到目前的缺陷数	t_f	未来时间
c	到目前所纠正的缺陷数	n_p	当前时间的故障计数
$N-n$	尚未出现的缺陷数	λ_p	当前时间的故障率
n_f	故障计数	t_p	当前时间

指数模型强调其简单易用和与硬件可靠性框架的对应性，主要缺点是需要产品可运行，因此无法在软件开发的早期应用，不能用于早期可靠性评价。表 9-3 总结了不同的指数模型，包括假设和说明。

表 9-3 常用指数模型

模型	MTTF	Δn	Δt	假设
一般指数	$1/[k(N-c)]$	$k^{-1}\lambda_p/\lambda_f$	$k^{-1}\ln\left(\frac{\lambda_p}{\lambda_f}\right)$	故障的严重性和发现概率是等效的；故障率与需加纠正残余的故障数直接相关
Lloyd-Lipow	$1/[k(N-c)]$	$k^{-1}\lambda_p/\lambda_f$	$k^{-1}\ln\left(\frac{\lambda_p}{\lambda_f}\right)$	故障率与需检测的残余故障数直接相关
穆沙基本模型	—	$N/\lambda_0(\lambda_p-\lambda_f)$	$N/\lambda_0\ln(\lambda_p-\lambda_f)$	参考时间为 0（系统测试开始）时的初始故障率
穆沙对数模型	—	$f^{-1}\ln(\lambda_p-\lambda_f)$	$f^{-1}\left(\frac{1}{\lambda_f}-\frac{1}{\lambda_p}\right)$	某些故障比其他模型容易被发现，故障发现率指数下降
舒曼模型	$1/k\left[\text{SLOC}-\left(\frac{N}{\text{SLOC}}-\frac{C}{\text{SLOC}}\right)\right]$	$k^{-1}\lambda_p/\lambda_f$	$k^{-1}\ln\left(\frac{\lambda_p}{\lambda_f}\right)$	适应不同的产品规模，每个参数按源代码行数归一化，注：这里，SLOC（Source Lines of Code）表示源代码的行数
Goel-Okumoto	—	—	—	故障可能导致其他故障，故障不可能立即消除

注：其中 k 是比例常数， N 是固有故障数， C 是纠正的故障数， n 是发现的故障数

（1）一般指数模型

通常情况下，模型假定全部故障在发现的严重性和概率中是等效的，发现后立即纠正。假定故障率 k 与软件中剩余的故障数有直接关系，即 λ 是纠正的故障数 c 的函数：

$$\lambda = k(N - c)$$

(9-4)

其中 k 是比例常数。在实际应用中，从发现的故障率与纠正的故障数之比的斜率中估计 k 。为达到最终失效率 λ_f 所需检测的故障数的投影为：

$$\Delta n = (1/k)\lambda_p/\lambda_f$$

(9-5)

其中 k 是上面用过的比例常数。

为达到设计的故障率所必需的时间投影为：

$$\Delta t = \left(\frac{1}{k}\right)\ln(\lambda_p/\lambda_f)$$

(9-6)

(2) Lloyd-Lipow 模型

Lloyd-Lipow 指数模型同样假定全部故障的严重性和发现概率是等同的。与一般指数模型不同的是, 假定故障率 λ 与软件中需检测 (不是纠正) 的残余故障数直接相关, 即 λ 是发现的故障数 n 的函数:

$$\lambda = k(N - c) \quad (9-7)$$

平均失效前时间 (MTTF) 的表达式、 Δn 和 Δt 与一般指数模型相同。

(3) 穆沙基本模型

穆沙基本模型是一般指数模型的另一种形式。利用初始 (即软件测试开始时) 故障率 λ_0 , λ_0 或者根据数据估计, 或者按 $\lambda_0 = N/k$ 计算, k 为先前引用的斜率值。在该模型中, 发现 n 个故障后的故障率是原始故障率的一小部分:

$$\lambda_n = \lambda_0 \left(1 - \frac{n}{v} \right) \quad (9-8)$$

其中 n 通常用 μ 表示, 而 u 用 v 表示, 因此时间 t 的故障率表达式为:

$$\lambda_t = \lambda_0 \exp \left[- \left(\frac{\lambda_0}{v} \right) \tau \right] \quad (9-9)$$

其中 $v = N/B$, N 是固有故障数, B 是故障降低比, 通常假定为 95% (即交付时未发现的故障的 95% 在交付后变为失效), τ 为系统测试时间。

为达到最终失效率 λ_f , 必须发现的故障数的映射为:

$$\Delta n = N / \lambda_0 (\lambda_p - \lambda_f) \quad (9-10)$$

为达到映射的失效率必须的时间映射为:

$$\Delta t = N / \lambda_0 \ln(\lambda_p - \lambda_f) \quad (9-11)$$

该模型的缺点是对背离假定非常敏感。另外, 参照穆沙前面的工作, 要注意单位是执行时间, 而不是日历时间。

(4) 穆沙对数模型

穆沙对数模型与其他指数模型的假定不同:

- 某些故障比其他的模型容易被发现。
- 故障检测率不是常数, 呈指数递减。

在该模型中, 发现 n 个故障后的故障率是原始故障率的函数:

$$\lambda_n = \lambda_0 \exp(-fn) \quad (9-12)$$

因此时间 t 处的故障率表达式为:

$$\lambda_t = \lambda_0 / (\lambda_0 ft + 1) \quad (9-13)$$

式中, f 是失效密度衰减参数, 是 n 后 n/t 的相关变化。

为达到最终失效率 λ_f ，必须发现的故障数的映射为：

$$\Delta n = 1/f \ln(\lambda_p / \lambda_f) \quad (9-14)$$

为达到映射的失效率必需的时间映射为：

$$\Delta t = 1/f(1/\lambda_p - 1/\lambda_f) \quad (9-15)$$

该模型的主要优点是不要求对 n 的估计。因为 f 可以在真实数据出现之前估计出来，该模型可用于在开发周期的早期估计可靠性。

与大多数指数模型一样，该模型的缺点是模型假定必须是有效的，结果才有效。特别是故障发现率呈指数递减并不为许多真实数据集所证实。另外，参照穆沙前面的工作要注意单位是执行时间，而不是日历时间，造成与硬件可靠性直接对比的困难。

(5) 舒曼模型

舒曼模型与一般指数模型类似，每个故障计数在该时间点按代码行数归一化。以前 $\lambda = k(N - c)$ ，这里是：

$$\lambda = kSLOC(N/SLOC - c/SLOC) \quad (9-16)$$

公式 $MTTF = 1/\lambda$ 中的 λ 采用舒曼模型表示。 Δn 和 Δt 的表达式与一般指数一样。该模型的优点是适应不同的软件产品规模。缺点是只能在 SLOC 确定之后的开发晚期应用，而此时一般指数的假定可能不适用。

(6) Goel- Okumoto 模型

该模型与其他指数模型不同，因为它假定故障可能引起其他故障，并且不能立即清除。要求迭代的解，模型的表达式是：

$$\lambda_t = ab \exp(-bt) \quad (9-17)$$

其中 a 和 b 可从下式迭代解出：

$$\begin{aligned} n/a &= 1 - \exp(-bt) \\ n/b &= at \exp(-bt) + \sum_{i=1}^n t_i \end{aligned} \quad (9-18)$$

利用 N 和 k 作为开始点，同时解这两个等式。

该模型的主要优点是可以比其他指数模型较早应用，而缺点是对背离假定非常敏感。

2. 基于威布尔分布的统计模型

威布尔分布模型是较早应用于软件的模型之一，它与用于硬件时的形式相同，有两个参数：尺度参数 a ($a > 0$) 和形状参数 b ： $b > 1$ 时，失效率增加； $b < 1$ 时，失效率降低； $b = 1$ 时，失效率为常数。到下一个失效的平均时间为：

$$MTTF = (b/a)\Gamma(1/a) \quad (9-19)$$

时间 t 处的可靠度为：

$$R(t) = \exp\left[-(t/b)^\alpha\right] \quad (9-20)$$

威布尔模型的优点是它弹性地考虑增加和减少失效率。缺点是在估计参数时比指数模型要多做很多工作。

3. 基于贝叶斯方法的统计模型

贝叶斯方法不关注估计的固有故障计数 N ，而是关注故障/失效率。经典法是假定可靠性和失效率为发现故障的函数，而贝叶斯方法假定无故障运行的软件程序是最可靠的。贝叶斯法另一个不同点是利用“先验知识”进行估计（因此有时被称为“主观”法）。

Thompson 和 Chelson 模型假定：

- 软件是可运行的。
- 软件故障率 λ 是未知的，假定软件故障的发生服从 Gamma 分布，参数为 X_i 和 f_i+1 。
- 故障在测试周期之间被纠正，而不是在测试期间纠正。
- 在单一测试（长度为 t_i ）期间发现的故障总数服从参数为 λt_i 的泊松分布。

该模型假定有 i 个测试周期，每个长为 t_i ；在本周期内发现的故障数用 f_i 表示。主观信息已作为周期 0 发生的事件插入中，即 t_o 和 f_o 代表先验信息。假如没有先验信息，这些值设为 0。如果有大量经验， t_o 可能非常大，特别是相对于期望评价时间；先验故障数的值也与过去的经验有关，而与先验时间无关。

令 T_i 表示全范围内所有测试周期长度的累积，即从周期 0 到 t_i ；令 F_i 表示全范围内所有故障 f_i 的累积，即从周期 0 到 i 。

那么 t 时间（ i 区间内）的可靠性表示为从前一个区间（ $i-1$ ）中以及目前第 i 区间得到的数据的函数：

$$R(t) = [T_{i-1}/(T_{i-1} + t)]^{F_{i-1}} \quad (9-21)$$

区间 i 的失效率估计为：

$$\lambda(t) = (F_{i-1} + 1)/T_{i-1} \quad (9-22)$$

该模型的优点与其假定有关：不假设 N 是固定的；可靠性不是 N 的直接函数；不假定故障立即得到纠正；贝叶斯模型的缺点是不能普遍地接受，因为它允许包含反映分析家相信失效率程度的先验信息。

4. 基于测试覆盖率的统计模型

测试覆盖率的倡议者将软件可靠性定义为已成功验证或测试的软件产品总量的

函数。下面讨论这种度量的 3 种形式：第一种是基于在最终接收测试期间成功测试率的简单比例，第二种和第三种度量是基于综合白盒子和黑盒子测试结果的方法。

该方法的倡议者认为，数据是从测试中收集和跟踪得到的，因此度量是可接受的，不需要附加验证。然而，可靠性工程师却认为这些方法与描述硬件可靠性的方法完全不同，这些度量方法都不涉及失效率或平均失效间隔时间等硬件可靠性的常用参数。

测试合格可靠性法把可靠性简单地定义为：在接受（黑盒子）测试中成功进行的测试用例数（用 s 表示）与执行的测试用例总数（用 r 表示）的比例：

$$R=s/r \quad (9-23)$$

结果的有效性决定于 r 的大小和代表软件全部运行轮廓的 r 的能力。在测试的后期，即将交付之前，可应用该模型接收或拒收软件。

IEEE 测试覆盖率可靠性方法假定可靠性依赖于已测试（黑盒）的功能和已测试（白盒）的程序两方面。假定为完成测试覆盖率必须进行所有类型的测试。可靠性定义为两个比例的乘积，以百分比表示：

$$R=p(\text{测试功能}) * p(\text{测试程序}) * 100\% \quad (9-24)$$

式中， $p(\text{测试功能})$ 是测试的性能数/总性能数。

Leone 测试覆盖率可靠性类似于 IEEE 模型，但是它假定只有白盒子或黑盒子测试可能分出可靠性级别，估计了两个白盒子变量 a 和 b 。两个黑盒子变量 c 和 d ，可靠性是 4 个比例的加权之和：

$$R=((a * w_1) + (b * w_2) + (c * w_3) + (d * w_4)) / (w_1 + w_2 + w_3 + w_4) \quad (9-25)$$

式中， a 是测试的独立路径数/总路径数； b 是测试的输入数/总输入数； c 是验证的功能数/总功能数； d 是访问的失效模式数/总失效模式数； w_1, w_2, w_3, w_4 的值代表权重，如果所有参数同样重要，这些权重值设为 1，如果有数据证明某些参数比其他的重要，则较重要的参数会获得较高的权重。

该模型包含了两个潜在的假定：第一是利用测试程序中的信息识别独立路径；第二是利用故障树分析（FTA）或失效模式、影响和危害性分析（FMECA）识别失效模式。

5. 利用跟随法的统计模型

利用跟随法估计基于测试中的观察软件中的故障总数 N ，利用播种法，即为了估计故障总数，将故障引入软件，然后确定测试期间发现多少这种故障的一种方法。为了解释，假设感兴趣的是池塘中鱼的数量 N 。一种估计方法是捉住 T 条鱼并做标志，然后放回池塘。下次再捉鱼时有标签的鱼数为 t ，没有标签的鱼数为 u 。未做标签的总鱼数为 U 。利用比例式 $u/U = t/T$ 估计，得到估计的总鱼数 $N=U+T$ 。

软件故障估计的基本播种法所用的步骤是：



- ① 识别一组故障，代表了在运行中发现的典型故障。
- ② 在测试人员和开发人员不知道的情况下给软件注入故障，总数为 T 。
- ③ 测试软件并识别发现的全部故障，令 t =发现的注入故障数， u =发现的非注入故障数。

④ 估计的非注入故障总数设为 U : $u/U = t/T$ 。

⑤ 估计的总故障数为 $N=U+T$ 。

⑥ 消除注入的故障。

通常不推荐这种方法，理由如下：

- 如何识别运行中的典型故障，并以完全随机的方式注入（无偏）？
- 播种假定故障是由编码错误引起的。由于要求、设计和维护错误引起的故障如何处理？
- 在典型的测试周期中，故障被纠正。注入故障可以在此过程中纠正吗？或在较晚的时候纠正？
- 种子故障是否会妨碍真实的故障被发现？
- 当维护人员排除注入的故障时如何对有意注入故障保密？如何证明花费资源注入故障是正当的？
- 在测试结束后如何做才能恢复没有注入故障的版本（并且没有纠正真正的故障）或消除（希望是全部）注入的故障？

一种替换性的双测试组法类似于基本播种法，只是要两个组。它假定：

- 两个独立的测试组在同一时间对同一软件进行测试。
- 两个组不共享测试中发现的故障信息。
- 两个组分别制订自己的测试计划，但对相同的软件功能进行测试。
- 两个组的经验和能力是相同的。

该模型基于 3 个数 n_1, n_2, n_{12} 预计总故障数 N ，其中 n_1 和 n_2 分别代表 1 组和 2 组发现的故障数， n_{12} 是两级都发现的故障数。

总故障数 N 的估计是：

$$N = R + n_1 + n_2 + n_{12} \quad (9-26)$$

其中 R 是估计的残余故障总数。

这种模型假定，随着两个组发现的故障数增多，残余故障数就减少。随着测试持续进行，假定 n_{12} 将增多。这就意味着，当软件中残留的故障越来越少时（即 R 趋近 0 时），两个测试组将开始发现同样的故障。然而，由于两个测试组可能都是无效的，可能不出现上述情况。基本的设想也可能不是切实可行的。组建两个完全独立的具有相同经验和能力的测试组并不总是可能的或经济的。

9.5.2 模型评价

目前得到公认模型准确性评价方法主要有：PL 检验法、U-结构图分析法、Y-结构图分析法等。

1. PL 检验法

PL (Prequential Likelihood) 检验法，即序列似然度比率分析法，认为软件失效时间的分布函数密度大的地方，软件发生失效的概率大，换句话说，预测软件失效时间的分布函数密度大的预测相比较而言更接近于真实。

设软件失效时间的概率密度函数为 $f_i(t)$ ，则 PL 定义为它的估计 $f'_i(t)$ ，即在实际观测值 t_i 上估计的预测密度。进行完 $n+1$ 次预测后，PL 进一步定义为 $n+1$ 个 PL 的简单乘积：

$$PL_{(n+1)} = \prod_{j=1}^{i+n} f'_j(t_j) \quad (9-27)$$

定义 PLR 为两个不同的预测系统 A 和预测系统 B 的 PL 的比值：

$$PLR = \frac{PL_{(n+1)}^A}{PL_{(n+1)}^B} = \prod_{j=1}^{i+n} \frac{f_j'^A(t_j)}{f_j'^B(t_j)} \quad (9-28)$$

其中， $f_j'^A(t_j)$ 和 $f_j'^B(t_j)$ 分别表示预测系统 A 和 B 的预测密度。若 $PLR \rightarrow \infty$ ，则预测系统 A 优于预测系统 B；若 $PLR \rightarrow 0$ ，则预测系统 A 与预测系统 B 是等价的，即二者产生的预测结果是等价的。

2. U-结构图分析法

设 $F_i(t)$ 为软件故障时间 T_i 的累积分布函数， $F'_i(t)$ 为以预测系统为基础获得的分布。U-结构图可判断 $F'_i(t)$ 是否平均地接近于实际分布 $F_i(t)$ 。设 t_1, t_2, \dots, t_{j-1} 为故障连续间隔时间，如果 $F'_i(t)$ 是 T_i 的真实累积分布函数，则 $u_i = F'_i(t)$ 称为满足均匀分布 $U(0,1)$ 的随机变量的一个实现，即预测分布与真实分布相同时，随机变量 u_i 将均匀分布在 $U(0,1)$ 的 $n+1$ 个随机变量的实现。因此，如果 $\{u_i\}$ 是靠近独立恒同分布 $U(0,1)$ 的，那么 $F'_i(t)$ 就是靠近 $F_i(t)$ 的。

U-结构图表示 $\{u_i\}$ 的样本累计分布函数与 $U(0,1)$ 的累计分布函数的接近程度。 $U(0,1)$ 的累计分布函数为以单位斜率通过原点的直线， $\{u_i\}$ 的样本累计分布函数是定义在区间 $(0,1)$ 上的阶梯函数，从 0 开始增长，增量为每步增加 $1/(n+1)$ 的 $n+1$ 个次序统计量。U-结构图将 $n+1$ 个 $\{u_i\}$ 升序分类，分类后的序列 ($j=0, 2, \dots, n$) 用 $\{u_j\}$ 表示，将点 $(u_j, \frac{j}{n} + 1)$ 描在图上，并绘制过原点斜率为 1 的直线（单元斜率曲线），如图 9-3 所示。

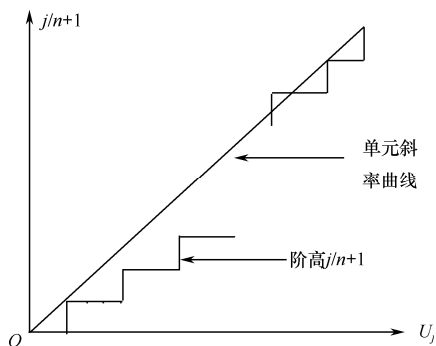


图 9-3 U-结构图示例

由上述分析可知, 预测分布越接近真实分布, 预测序列结构图就越接近单元斜率曲线。预测序列结构图与单元斜率曲线的偏离表明存在非一致性, 且预测序列的结构图和单位斜率曲线的最大垂直距离 (Kolmogorow-Smimov, KS 距离) 就是预测分布与真实分布相距多远的一个测度, KS 距离越大, 表明偏差越大。总之, U-结构图与单位斜率线之间的偏离表明预测存在着某种偏差, 当 U 结构图比单位斜率线高时, 表明预测过于乐观, 反之, 则表明预测较悲观。U-结构图法与预测分布的整体形状有关, 而不是仅局限于个别点的分析, 因此更具有一般性, 可用来分析预测分布与真实分布的系统差别。

3. Y-结构图分析法

Y-结构图用于表示模型偏差趋势, 它能够检测出 U-结构图是否掩盖了模型的一致偏差。例如, 对某一特定预测系统, 在 U-结构图中的某一阶段预测趋势乐观, 而另一阶段则趋势悲观, 但由于其前后特性互补, U-结构图得到的 KS 值可能还是较小。使用 Y-结构图则可以检测出序列 $\{u_i\}$ 的变化趋势。

Y-图要求对 $\{u_i\}$ 进行如下变换:

$$x_j = \ln(1 - u_j), j = i, i+1, \dots, i+n \quad (9-29)$$

$$y_j = \sum_{l=i}^j x_l / \sum_{l=i}^{i+n} t_l, j = i, i+1, \dots, i+n \quad (9-30)$$

当 u 值均满足独立恒同均匀分布 $U(0,1)$ 时, y 值是 n 个满足独立恒同均匀分布 $U(0,1)$ 的次序统计量。Y-结构图表示 $\{y_i\}$ 的样本累计分布函数与单位斜率线的接近程度。Y-结构图与 U-结构图相同, 将点 $(y_j, \frac{j}{n} + 1)$ 描在图上, 并绘制过原点斜率为 1 的直线, 此时单位斜率线上产生的偏差表示预测趋势。模型偏差趋势同样用 Y-结构图中的 KS 距离表示, KS 距离越小, 模型偏差趋势越小。

PL 检验法是一种用于比较不同预测系统的相对准确性的常用方法, 但它不能说明某一预测系统是否客观准确。U-结构图分析法是在概括 PL 简单的平均时间检验的

基础上形成的,用来判断预测分布是否平均地接近于实际分布,但是它无法检测 u_i 的变化趋势。Y-结构图将 u_i 经函数变换,弥补了U-结构图的不足,能够检测出U-结构图可能掩盖的模型一致偏差。总之,如果在一系列可供选择的模型中选择一个时,可使用PL检验法找出一个相对而言比其他模型更准确的模型,但是还需要经过U-结构图分析法和Y-结构图分析法的进一步论证此模型预测结果的精确性。

9.6 软件可靠性设计

为了保证软件的可靠性,在软件设计开发过程中,应该遵循以下准则:

① 软件开发规范化。应将软件开发过程分为若干个阶段,每个阶段编制必要的文档并进行检查、分析和评审,实行配置管理。

② 尽可能采用先进、适用的软件开发工具,并确保软件开发工具免受计算机病毒侵害。

③ 加强软件检查和测试。应尽早开展软件检查和测试,采取措施(如自检、互检、专检相结合的“三检制”,制订设计检查单等)使检查工作切实有效,软件测试应达到规定的要求。

④ 对具有高可靠性和安全性要求的功能,应权衡用硬件实现还是用软件实现的利弊,做出妥善决策。

⑤ 软件的可靠性指标应与硬件的可靠性指标大体相当,可根据具体情况进行适当的调整,但调整不宜过大,并且所分配的指标应能验证。

⑥ 在系统控制回路中,安全关键功能的执行在可能时必须经操作人员确认或启动。

⑦ 在安全性较为关键的计算机系统中,应当设计一个称为安全性内核的独立计算机程序,用来监视系统并防止系统进入不安全状态。当出现潜在不安全的系统状态或者有可能转移到这种状态时,它将系统转移到规定的安全状态。

⑧ 必须采取措施保证自动记录检测出的所有系统故障及系统运行情况。

⑨ 禁止回避检测出的不安全状态。在系统设计时考虑故障的自动检测,一旦检测出不安全状态,系统应做出正确响应,不得回避。

⑩ 软件应进行保密性设计,保证系统设计应能防止越权,或意外地存取、修改软件。

⑪ 软件应进行容错设计。对可靠性要求很高的系统应同时考虑硬件和软件的容错设计,而不能只考虑硬件容错设计。

⑫ 下述软件应定为关键软件。



- 故障检测的优先级结构及安全性控制，或校正逻辑、处理和响应故障的模块。
- 中断处理程序、中断优先级模式，以及允许或禁止中断的例行程序。
- 产生对硬件进行自主控制信号的软件。
- 产生直接影响硬件部件运动或启动安全关键功能的信号的软件。
- 其输出是显示安全关键硬件的状态的软件。

⑬ 嵌入式软件的运行过程与相关系统硬件的运行过程相互交错，密不可分，设计因素相互影响。在进行软件可靠性和安全性设计时必须考虑与硬件设计有关的要求。

⑭ 对安全关键软件而言，应在软件开发的各个阶段进行有关的软件危险分析。

⑮ 对关键软件功能的设计。

- 安全关键功能必须至少受控于两个独立的功能。
- 安全关键的模块必须同其他模块隔离，安全关键的模块必须放在一起，以便对其进行保护。
- 安全关键功能必须具有强数据类型，不得使用一位的逻辑“0”或“1”来表示“安全”或“危险”状态，其判定条件不得依赖于全“0”或全“1”的输入。
- 安全关键的计时功能必须由计算机控制，使操作人员不能随意修改。
- 在启动安全关键功能之前，必须对可测试的安全关键单元进行实时检测。
- 当检测到不安全的情况时，软件必须采取措施对其进行处理，如软件无法处理这种情况，则应保证将控制转换到硬件的安全子系统。

⑯ 软件应进行简化设计、余量设计和防错程序设计。

⑰ 软件更改要求：

- 对软件的更改应执行配置管理规范，严格实施更改管理：对更改过的软件必须进行回归测试，确保对有关文档进行相应的更改，以保持文档的一致性。
- 禁止对已处于配置管理下的目标程序代码进行修补，所有的软件更改必须用源程序语言编码并编译。
- 对已经推广应用的或者在现场系统上的安全关键软件的更改，必须以修改后通过审查批准的整个软件形式来发布，而不得对目标程序代码进行修补。
- 对固件的更改应在软件更改经过验证之后进行，必须由二人或多人共同完成，必须以经过测试的全功能电路板的形式发布，该电路板的设计及安装过程应使由于误操作、静电放电、正常或异常的存储环境对电路造成损害的可能性极小。
- 关键软件必须采取保护措施。

下面具体说明如何贯彻上述设计准则，开展软件可靠性设计。

1. 异常计算的设计

在数值计算中，要充分考虑计算中的异常情况，如：在除法计算中，要考虑除数为 0 或很小时的计算溢出处理，可在计算前先进行除数大小的判别检查，即在计算 $1/x$ 时，一定要判断 x 是否为 0。在开平方根（偶次方根）的计算中，要考虑被开根数是否大于等于零，可在计算前先进行被开根数的符号判别。

2. 安全关键信息码的设计

安全关键信息码应采用具有检错能力的编码。

禁止对关键信息用一位的逻辑判别，如用“0”来表示“关闭设备”，用“1”来表示“启动设备”。对此具有检错能力的编码可以用二位的逻辑判别，如用“01”来表示“关闭设备”，用“10”来表示“启动设备”。显然在有一位可能受干扰的系统假设下，用一位的逻辑判别无法检测其是否受干扰，而二位的逻辑判别则可以检测其是否受干扰，如“00”和“11”就表示信号受到了干扰。

3. 接口数据的定义

在通信接口数据定义时必须明确通信的数据量、数据格式、数据内容、换算要求、传输协议、传输率、误码率。

依据双方计算机的字长设计双方方便的交换字格式，如中心机字长是 32 位，而信号处理机是 16 位，则涉及信号处理的交换字应以 16 位为一个独立信息单位进行定义。不要使信号处理机依靠 2 个字的部分信息（如第 1 字的后 6 位和第 2 字的前 10 位）组合来完成一个独立信息的解释。

4. 人机交互误操作的防范和处理

软件人机界面的设计要充分考虑误操作的防范和处理。

屏蔽不期望的操作项，如“功能 2”键的操作必须是在“功能 1”键的操作通过后方可进行，当未按“功能 1”键或按后尚未通过时，“功能 2”键是不可按的。

对关键操作要增加“确定”和“取消”的再次选择框，如按“系统退出”键后，应弹出“确定”和“取消”的再次核实对话框，以免误按“系统退出”键后系统误退出。

5. 异常处理的设计

软件编程不能只考虑正常情况下的处理，还应充分考虑可能的异常事件的处理。在软件的设计过程中应专门对可能的异常事件进行分析，这一工作称之为“软件失效模式及影响分析”。例如，在对数据文件操作时可以考虑的异常事件有：

- ① 错误的文件名或文件数。



- ② 文件没找到。
- ③ 错误的文件模式。
- ④ 文件已经被打开。
- ⑤ I/O 设备错误。
- ⑥ 文件已经存在。
- ⑦ 错误的记录长度。
- ⑧ 磁盘满。
- ⑨ 超过文件结尾的输入。
- ⑩ 错误的记录数。
- ⑪ 错误的文件名。
- ⑫ 太多的文件。
- ⑬ 设备不可使用。
- ⑭ 权限不允许。
- ⑮ 磁盘没准备好。
- ⑯ 不能对不同设备重新命名。
- ⑰ 路径或文件访问错误。
- ⑱ 没找到路径。

显然，以上 18 种情形无需也不必都考虑，可依据实际情况进行相应的裁剪，如在人机交互软件中用户选择数据文件，则“错误的文件名或文件数”、“文件没找到”和“路径或文件访问错误”是必须要考虑的，需要对此设计相应的处理方法。

6. 错误陷阱的使用

一些高级语言，如 Visual Basic、Visual C、Ada 等，都具有运行错误陷阱功能。例如，在 Visual Basic 6.0 中的 On Error 语句，可以启动一个错误处理程序并指定该子程序在一个过程中的位置。

软件可靠性的设计方法很多，上面只列举了一部分，其他的方法，如防程序死循环设计、模块单一出口设计、软件多路冗余和多版本冗余设计等，读者可参阅相关文献资料。

9.7 软件可靠性分配

9.7.1 考虑因素

软件可靠性分配与硬件的可靠性分配原理是相似的，也是主要以失效率作为指

标,但考虑的因素不同。从工程应用的角度看,软件可靠性分配至少应该考虑以下因素:重要度系数、调用系数、复杂度系数。

1. 重要度系数 U_i

把软件系统的可靠性指标分配到各软件子系统时,首先必须考虑子系统的重要度。子系统的重要度是指子系统发生失效对系统功能的影响程度。子系统 i 的重要度系数用 U_i 表示。 U_i 可以通过工程分析(例如 FMECA 分析)确定。一般地, $0 < U_i \leq 1$ 。如果子系统 i 的失效将使系统失效或造成更严重的效果,则 U_i 可取值为 1。

2. 调用系数 D_i

软件与硬件的工作状态不同:硬件工作时,各部件通常都处于工作状态;而软件运行时,各子系统一般是逐个调用的,在软件系统的运行时间中,各子系统的运行时间是不同的。我们用调用系数 D_i 表示子系统 i 的调用情况。

调用系数 D_i 可以定义为:

$$D_i = \frac{t_i}{T} \quad (9-31)$$

在上述公式中, T 是软件系统的运行时间; t_i 是在软件系统运行时间 T 中第 i 个子系统的运行时间。

调用系数 D_i 这一定义虽然准确,但在软件开发的初期,软件产品处于规划和设计阶段,各个子系统、模块的运行时间无法确定,因此,我们可以得到对调用系数 D_i 的近似定义式:

$$D_i = \frac{W_i}{W} \quad (9-32)$$

$$W = \sum_{i=1}^n W_i \quad (9-33)$$

式中, W_i 是第 i 个子系统被调用的次数; W 是各子系统被调用次数的总和。这一近似定义式蕴含了各个子系统的运行时间相同的假设,这是一种近似假设。有了这一假设,在软件开发的初期就可以根据经验估计出各个子系统的调用次数,从而获得调用系数 D_i 的近似值。

3. 复杂度系数 C_i

子系统复杂性越大,其设计难度和发生错误的可能性就越大。这一因素在软件可靠性分配时必须考虑,否则将使复杂性高的子系统设计人员无法实现预期的可靠性要求;而复杂性低的子系统较易达到要求。我们用 C_i 表示子系统 i 的复杂度系数。复杂度系数的确定方法可以借鉴软件工程中软件复杂性度量的概念。将各软件子系统的复杂性度量经过变换得到子系统的复杂度系数:



$$C_i = \frac{CX_i}{\sum_{i=1}^n CX_i} \quad (9-34)$$

在上式中, CX_i 是软件复杂性度量中的普遍标识, 它可以是 Halstead 度量、McCabe 度量、Thayer 度量或其他度量。在实际使用上式时, 必须确定选择哪一种复杂性度量, 这主要依据分析人员拥有的信息量和以往的工程经验:

- 一般而言, 在系统开发早期, 分析人员掌握的信息非常有限, 这时不妨首先对各个子系统的指令数进行粗略的估计, 用估计的指令数作为复杂性度量, 进行可靠性预分配。这一做法虽然略显粗糙, 却十分有用。
- 在开发过程进入详细设计阶段, 分析人员掌握了各个子系统使用的操作符和操作数的信息时, 可以用 Halstead 复杂性度量对预分配加以调整。Halstead 复杂性度量比指令数度量更能反映程序的特征, 这种方法得到的复杂度系数更趋合理。当然, 您也可以选用 McCabe 复杂性度量等其他方法。

软件复杂性度量的方法在普通的软件工程资料中都可以找到, 这里就不再赘述了。复杂性越高的子系统, 其复杂度系数越大。不难看出, 复杂度系数满足下式:

$$\sum_{i=1}^n C_i = 1 \quad (9-35)$$

9.7.2 基本公式

有了上述系数的定义, 软件可靠性分配的基本关系式可以用下式表示:

$$\lambda_i = \frac{C_i}{U_i D_i} \lambda_s \quad (9-36)$$

式中, λ_i 是分配给第 i 个软件子系统的失效率, λ_s 是软件系统的失效率指标。

必须说明的是: 上式只适用于软件系统的可靠性分配。对于包含硬件和软件的系统来说, 如何合理分配硬件和软件的可靠性指标, 主要依靠以往类似系统的工程经验。

9.8 软件可靠性预计

目前许多软件的可靠性模型和方法都是针对软件生存周期中的后期的。遗憾的是, 对于适合于早期进行可靠性预测的研究, 却很少见。从工程实用的角度看, 在

软件开发初期预测软件的可靠性比在软件生存期的后期估计软件的可靠性更有意义。目前对软件可靠性预计方法主要分为两类：基于模型的软件可靠性预计和基于经验公式的软件可靠性预计。

9.8.1 基于模型的软件可靠性预计

软件可靠性基本的预计模型包括利用组织的内部数据，根据广泛的经验和跟踪进行预计，主要有 3 类可靠性预计模型：穆沙执行时间模型、普特内姆模型和米尔模型。

1. 穆沙 (Musa) 执行时间模型

该模型由贝尔实验室的 John Musa 于 20 世纪 70 年代中期开发，是最早的软件可靠性预计模型之一。穆沙模型利用程序执行时间作为独立变量，简化的穆沙模型是：

$$n = N_0 \left[1 - \exp \left(\frac{-Ct}{N_0 T_0} \right) \right] \quad (9-37)$$

$$T = T_0 \exp \left(\frac{Ct}{N_0 T_0} \right) \quad (9-38)$$

$$R(t) = \exp \left(\frac{-t}{T} \right) \quad (9-39)$$

式中 N_0 是固有的错误数， T_0 是测试开始时的 MTTF (故障前平均工作时间)，而 C 是“检查压缩因子”，它等于等效工作时间与测试时间之比：

从这些关系式中我们可以导出必须发现及校正的故障数，或者从 T_1 提高到 T_2 需要的程序执行时间：

$$\Delta n = N_0 T_0 \left(\frac{1}{T_1} - \frac{1}{T_2} \right) \quad (9-40)$$

$$\Delta t = \left(\frac{N_0 T_0}{C} \right) \ln \left(\frac{T_2}{T_1} \right) \quad (9-41)$$

假设一个大的程序含有大约 300 个错误，在开始检查时记录的 MTTF 为 1.5 小时，压缩因子为 4，要把残余的错误数减少到 10 应当进行多少次检查？在 50 小时的运行中的可靠度是多少？

由上述公式，可以得到：

$$\Delta n = (300 - 10) = 300 \times 1.5 \left(\frac{1}{1.5} - \frac{1}{T_2} \right)$$

$$T_2 = 45 \text{ 小时}$$

$$\Delta t = \left(\frac{300 \times 1.5}{4} \right) \cdot \ln \left(\frac{T_2}{1.5} \right)$$

$$\Delta t = 382.6 \text{ 小时}$$

$$R_{50} = \exp \left(\frac{-50}{45} \right) = 0.33$$

2. 普特内姆 (Rayleigh) 模型

普特内姆模型最早在 1978 年被提出，模型认为软件项目遵循由动态多变量密度曲线描述的成本估算模型。Gaffney 提出软件质量评估的缺陷技术应给予开发过程的六个阶段（概要设计、详细设计、编码、单元测试、集成测试、系统测试），并认为六个阶段在开发过程中的缺陷模式遵循 Rayleigh 曲线。

Rayleigh 模型是 Weibull 分布家族的一个成员，其标志性特性之一就是其概率密度的尾部逐渐趋于零，但达不到零，表达式记为：

$$f(t) = 2 \times \alpha \times k \times t \times \exp(-\alpha t^2) \tag{9-42}$$

其中， k 和 α 是根据数据拟合的常数， t 是时间，单位为月。Rayleigh 进一步开发了一个顺序进度（并不等同于其实时间），以此表示开发过程中的里程碑，参见表 9-4。

表 9-4 普特内姆时间轴里程碑

里程碑号	里程碑	里程碑号	里程碑
0	可行性研究	5	用户系统测试开始
1	初步设计评审，完成功能设计	6	初始运行能力，安装
2	关键设计评审，完成详细设计	7	全部运行能力，里程碑程序应用中可靠性大约为 95%
3	完成原始代码	8	完成应力测试，可靠性达到 99%
4	系统集成测试开始	9	假定已调试，可靠性达到 99.9%

表 9-4 中关键的第 7 里程碑用 t_d 表示，对应开发阶段的结束和全操作能力的开始，该点被定义为在 95 百分点（即到该点时，软件开发中的全部缺陷的 95% 已被发现）。利用 t_d 作为参考基准，它又用 N 和 t_d 表示模型常数符号 α 和 k ，预计每月（进度表月份的函数）的期望缺陷数和固有缺陷总数 N 的公式如下：

$$f(t) = (6N/t_d^2) \times t \times \exp(-3 \times t^2/t_d^2) \tag{9-43}$$

【例 9-1】 一个基于 FORTRAN 开发的程序，计划在 10 个日历月时全面运行（到达里程碑 7），导出 t_d^2 为 100。计算开发期间每月的期望缺陷数可得：

$$f(t)=0.06N\times t\times \exp(-0.03t^2)$$

(9-44)

图 9-4 给出了计算结果，其中 t 是月份数， $f(t)$ 是第 t 个月内发现的总缺陷数的期望比例，而 $F(t)$ 代表累积比例。同时画出计划的开发进度表的里程碑数做比较；对应 95 百分点的第 7 里程碑实际在第 10 个月，对应 99 百分点的第 8 里程碑在进度表的第 13 个月，对应 0.999 的里程碑 9 在进度表结束的第 15 个月时尚未达到。

与穆沙模型仅在系统测试开始（即里程碑 4）时进行预计相比，该模型的一个很大优势是可以在开发过程中的不同点预计期望的故障数。

该模型还给出了到下一个缺陷的平均时间 $MTTD=1/f(t)$ ，只是在里程碑 4 后这个指标才有意义（在里程碑 4 之前，系统不可能开发出那么多可检测出的缺陷数），MTTD 随着缺陷的逐渐消除而增长。

t	$f(t)$	$F(t)$	Mile
1	0.058	0.058	
2	0.106	0.165	1
3	0.137	0.302	
4	0.149	0.451	2
5	0.142	0.592	
6	0.122	0.715	3
7	0.097	0.811	4
8	0.07	0.881	5
9	0.048	0.929	6
10	0.03	0.959	7
11	0.017	0.976	
12	0.01	0.986	
13	0.005	0.991	8
14	0.002	0.993	
15	0.001	0.994	

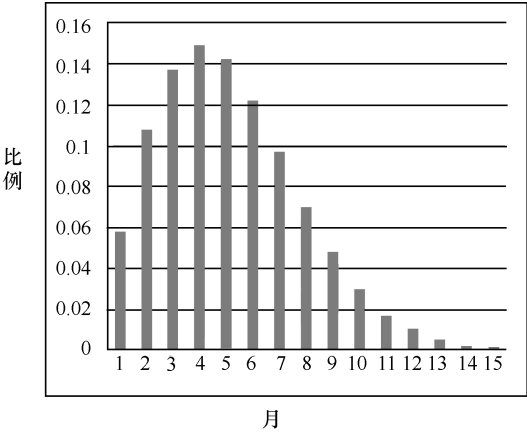


图 9-4 预期的缺陷总数的比例

3. 米尔模型

米尔提出了另一种软件可靠性预计的方法。这是一种更为实用的方法，将已知数目的错误故意加入程序中，当完成调试（检验及/或检查）时，记录表示发现了多少“加入”的错误。残余的未知错误数被假设是被发现的与残余的“加入”错误之比的函数：

$$n=N_0\left[1-\exp\left(\frac{-n_s}{N_s-n_s}\right)\right]$$

(9-45)

式中的 N_s 是“加入”错误的总数，而 n_s 是残余的“加入”错误数。

【例 9-2】残余错误数的估算

经验表明，一个程序在验证开始时可能包含有大约 100 个错误，故意加入 10

个错误，并尽可能地随机安排，其中 9 个错误在验证结束时发现。有多少个原有的错误可能残留下来？

$$n = 100 \left[1 - \exp \left(-\frac{1}{10-1} \right) \right] = 10.5 \quad (9-46)$$

即大约有 10 或 11 个错误。

米尔方法避免了时间问题。但明显的实际缺点是必须停止试验来校正故意加入的错误。为了获得确切的残余错误数的预计值，“加入”的错误必须是与固有错误的类型相同的错误，而且有同样的比例。这种方法很可能更适用于编码错误，因为，规范及设计误差的加入不是那么直接。然而，米尔方法尚未成为典型程序的实用方法，尽管它与用来校验/检查例行程序能力的方法相类似，这种例行程序用于诊断在硬件中故意引入的故障。

9.8.2 基于经验公式的软件可靠性预计

应用软件可靠性模型，无论从模型选取，还是从预计或估计的精度来讲都存在很多不足。另外由于许多模型的工程化程度较差，使用起来相当不方便，所以，在工程界逐渐产生了一种经验公式法。经验公式法的主要思路是：利用软件的一些基本特征、软件开发环境和应用类型来预计或估计软件可靠性。

在软件生命周期的早期预测软件可靠性的方法中，最早并且目前应用最为普遍的是美国 Rome 航空开发中心研究的经验公式与具体的软件可靠性模型相结合的方法，主要有两类模型：RL-TR-92-52 模型和 RL-TR-92-15 模型。

1. Rome 航空开发中心预计模型

(1) 模型 1: RL-TR-92-52

Rome 航空开发中心在其研究报告 RL-TR-92-52 中开发了对软件错误密度的预测方法，以及将其转换为另一种可靠性度量指标（如失效率）的方法。

Rome 航空开发中心的研究结果认为，软件的错误密度主要与如下因素有关：

① 软件的应用类型（如实时控制系统、科学计算系统或信息管理系统等），用 A 表示。

② 软件的开发环境（以开发方法学和可用工具进行说明），用 D 表示，开发环境类型包括结构模型、半联模型和嵌入式模型 3 种。

③ 要求和设计表示度量标准，包括：

- 非常规管理，用 SA 表示。
- 可归纳性，用 ST 表示。

- 向软件引入质量复审结果，用 SQ 表示。

④ 软件实现度量标准，包括：

- 编程语言类型（如汇编、宏汇编、高级语言等），用 SL 表示。
- 程序规模，用 SS 表示。
- 模块化，用 SM 表示。
- 可复用性范围，用 SU 表示。
- 复杂性，用 SX 表示。
- 对软件引入标准复审结果，用 SR 表示。

软件的初始错误密度（用 δ_0 表示）等于上述因子的乘积，即：

$$\delta_0 = A \times D \times (SA \times ST \times SQ) \times (SL \times SS \times SM \times SU \times SX \times SR) \tag{9-47}$$

模型中涉及的因数及典型取值可参见表 9-5。

表 9-5 预计模型的参数介绍

因 数	度 量	采用阶段	折中范围
A	在开发不同应用类型时的难度，用“缺陷数/KSLOC”表示，取值范围 2~14	A-T	不固定
D	开发组织、方法、工具、技术、文件，取值范围为 0.5~2.0	A-D-T	最大范围
SA	软件异常管理，容错设计指示，取 0.9~1.1	通常 C-T	小
ST	软件跟踪能力因数，要求的设计和代码跟踪能力，一般取 0.9~1.0	通常 C-T	大
SQ	软件质量，度量遵守的编码标准，参考取值 1.0~1.1	通常 C-T	小
SL	软件语言，按语言类型标准化故障密度	C-T	不适用
SX	软件复杂程度，单元复杂度度量，参考取值 0.8~1.5	C-T	大
SM	软件模块性，参考取值 0.9~2.0	C-T	大
SR	软件标准评审，设计规则符合性度量，参考取值 0.75~1.5	C-T	大
注：A 为概念或分析阶段；D 为详细设计和顶层设计阶段；C 为编码阶段；T 为测试阶段			

根据大量的历史信息，该模型被认为是少数公认有效的预计模型之一，该模型的优点包括：

- 当软件的概念已知时，就可以应用。
- 在概念阶段，允许利用 what-if 分析来确定开发环境对故障密度的影响。
- 在设计阶段，允许利用 what-if 分析来确定软件特性对故障密度的影响。
- 可以唯一地用于组成软件系统的每个应用类型，允许系统软件可靠性分配。



- 该预计可以根据特定的组织环境以往的软件数据，为 A、S 和 D 定制唯一的值。

该模型的缺陷有：

- 采用的因数和值均来自于为空军系统开发的软件，如果正在讨论的软件与空军应用类型不匹配，那么必须选择平均值。航空应用类型并不能很好地适应军事环境以外的开发软件。
- 采用 SLOC（源代码行数）作为规模量度，已越来越不适应软件开发技术的发展，例如图形用户界面 CGUD 系统的开发和商业现货 CCOTS 软件的应用。

(2) 模型 2: RL-TR-92-15

由 Hughes Aircraft 为 Rome 实验室提供的技术报告（编号：RL-TR-92-15）研究了许多软件系统，得出平均故障率预计值为 6 个故障/1000SLOC（这是穆沙执行时间模型采用的故障率缺省值）。另外，模型给出了 24 个预计因数，用于估计以下 3 个主要的变量：

- 在每个开发阶段（DP）中检测出的故障数。
- 在每个阶段中利用的人工时间（UT）。
- 产品的规模（S）。

估算模型为：

$f(DP)=18.04+0.05\times(0.009X_1+0.99X_2+0.10X_3-0.0001X_4+0.0005X_5)$ (9-48)

$f(UT)=17.9+0.04\times(0.007X_1+0.796X_2+0.08X_3-0.0003X_4+0.0003X_5+0.00009X_6+0.0043X_7+0.013X_8+0.6X_9+0.003X_{10})$ (9-49)

$f(S)=17.88+0.04\times(0.0007X_1+0.8X_3+0.01X_8+0.6X_9+0.008X_{23}+0.03X_{25})$ (9-50)

其中回归模型的变量系数和描述列在表 9-6 中。

表 9-6 回归因数及其说明

因数变量	变量描述	系 数		
		EQ ₁	EQ ₂	EQ ₃
X ₁	软件要求规范中的故障数	0.009	0.007	0.007
X ₂	规范中的要求陈述	0.99	0.796	NA
X ₃	规范的页数	0.1	0.08	0.8
X ₄	要求分析花费的人工时间（月）	0.0001	-0.0003	NA
X ₅	基线后要求的变更	0.0005	0.0003	NA
X ₆	初步设计文件中的故障数	NA	0.000 09	NA

(续表)

因数变量	变量描述	系 数		
		EQ ₁	EQ ₂	EQ ₃
X_7	CSCS 数	NA	0.004 3	NA
X_8	设计的单元数	NA	0.013	0.01
X_9	设计文件的页数	NA	0.6	0.6
X_{10}	初步设计花费的人工时间（月）	NA	0.003	NA
X_{11}	设计文件中的失效数	NA	NA	NA
X_{12}	详细设计花费的人工时间（月）	NA	NA	NA
X_{13}	基线后识别的设计故障数	NA	NA	NA
X_{14}	内部评审后识别的设计故障数	NA	NA	NA
X_{15}	可执行的 SLOC 数	NA	NA	NA
X_{16}	代码评审中发现的故障数	NA	NA	NA
X_{17}	程序员经验的平均数（年）	NA	NA	NA
X_{18}	评审的单元数	NA	NA	NA
X_{19}	每单元的平均 SLOC 数	NA	NA	NA
X_{20}	单元中的平均分支数	NA	NA	NA
X_{21}	包含的分值百分数	NA	NA	NA
X_{22}	平均嵌套深度	NA	NA	NA
X_{23}	单元被测试的次数	NA	NA	0.008
X_{24}	编码和单元测试花费的人工时间（月）	NA	NA	NA
X_{25}	等效的 ($X_{13}+X_{14}+X_{16}$)	NA	NA	0.03

模型的优点：

- 支持在系统测试前估计其可靠性。
- 模型考虑了费用、产品参数、故障和时间。

模型的缺点：

- 数据采集只来源于一个组织的一种行业/应用类型。
- 它没有揭示规范规模的度量单位。

2. 航空软件可靠性的预计模型

对于航空软件来说，通常有 6 种应用类型，应用类型不同，其平均故障密度也不同，如表 9-7 所示。表中的数据是统计数据，根据圆环系统的实际情况，在实际应用中可能需要做出某些调整。



表 9-7 不同应用类型的平均故障密度值

应用类型	平均故障密度	应用类型	平均故障密度
机载	0.0128	生产中枢	0.0085
战略	0.0092	开发/保障	0.0123
战术	0.0078	总平均	0.0094
过程控制	0.0018		

Musa 经过大量的统计数据，得到软件生存期各阶段开始时的平均错误密度，如表 9-8 所示。这些统计数据对估计各开发阶段的故障密度有重要的参考价值。

表 9-8 不同阶段的平均故障密度值

阶段	平均故障密度	阶段	平均故障密度
编码（编译/汇编后）	0.0995	系统测试	0.006 01
单元测试	0.0192	使用	0.001 48

一旦确定了初始密度，就可以通过下式求得软件的初始失效率（用 λ_0 表示）：

$$\lambda_0 = f \times K \times (\delta_0 \times I_s) \tag{9-51}$$

在上式中， f 为程序的线性执行频度，其值为程序的平均执行率 R 除以程序包含的目标指令数 I ，如下式所示； I_s 为程序源代码行数； K 为错误暴露比，根据 Musa 的统计结果，其均值为 4.20×10^{-7} ，并且满足： $1.4 \times 10^{-7} \leq K \leq 10.6 \times 10^{-7}$ 。

$$f = \frac{R}{I} \tag{9-52}$$

上式的目标指令数 I 的估计值可以由程序的源代码行数 I_s 乘以指令扩展率 Q_x 得到（ Q_x 的均值为 4.0；对于 C 语言开发的程序，取 $Q_x=2.5$ ）。这样，上式可以改写为：

$$f = \frac{R}{I_s * Q_x} \tag{9-53}$$

也可以使用已有的经验数值，如表 9-9 所示，将故障密度直接转换为故障率。

表 9-9 不同应用类型的故障密度与故障率转换因子

应用类型	转换率	应用类型	转换率
机载	6.2	过程控制	3.8
战略	1.2	生产中枢	23.0
战术	13.8	平均	10.6

有了软件的初始失效率，结合 Musa 执行时间模型，我们不难得到软件在执行一段时间 τ 后的失效率 $\lambda(\tau)$ 。

$$\lambda(\tau) = \lambda_0 * e^{-f * K * B * \tau} \tag{9-54}$$

上式中引入了错误递减因子 B ，它是错误减少率与故障发生率的比值。Musa 的统计数据表明， B 的均值为 0.955。 B 为不同值时的意义如下：

- $B>1$ ：在一次排错过程中排除了多个错误。
- $B=1$ ：一旦发现错误立即排除，以后此错误不再出现。
- $B<1$ ：在排错过程中引入新的错误。
- $B=0$ ：排错无效，错误无增减。
- $B<0$ ：排错后，错误反而增加了。

以上数据和模型适用于以下情况。

- 当用户希望在程序执行前和得到失效数据前做早期的可靠性预测。
- 当观测失效数据时，程序变化很大。
- 用户想了解新的软件工程技术对开发过程的影响。

参 考 文 献

- [1] 胡燕，朱明让，等. 可靠性设计大全. 北京：中国标准出版社，2006.
- [2] Stephen H.Kan 著，软件质量工程的度量与模型. 北京：机械工业出版社，2003.
- [3] 徐仁佐，谢旻，郑人杰. 软件可靠性模型及应用. 北京：清华大学出版社，1994.
- [4] GB/T 11 457-1989. 信息技术软件工程术语.
- [5] GJB 2786-1996. 军用软件开发通用要求.
- [6] NASA-GB-1704.13-1996. 安全关键软件的分析 and 开发指南.
- [7] 黄锡滋. 软件可靠性、安全性与质量保证. 北京：电子工业出版社，2002.
- [8] 徐仁佐. 软件可靠性工程. 北京：清华大学出版社，2007.
- [9] John D Musa. Software Reliability Engineering. 北京：机械工业出版社，2003
- [10] 丁操. 软件可靠性预计模型及其主要参数估计算法研究. 南京邮电大学硕士学位论文，2008.
- [11] 王纬. 软件工程与软件可靠性——第五讲软件可靠性工程实施方法. 质量与可靠性，2001，（5）.
- [12] 王纬. 软件工程与软件可靠性——第六讲软件可靠性工程实施中的几个技术问题. 质量与可靠性，2001，（5）.
- [13] 郑曦. 基于组件式软件系统的可靠性指标分配与预计模型. 华南理工大学硕士学位论文，2012.



- [14] 白凯丽, 宁静峰. 基于 PDCA 模型与 Rayleigh 模型的软件质量管理. 长春工业大学学报, 2013, (4): 416~421.
- [15] 周雷, 彭永怀, 刘章宇. 美国军用手册 338 中的软件可靠性预计模型及其应用. 电子质量, 2008, (5): 60~61.
- [16] 陈未如, 李可明. 基于架构的软件可靠性分配模型及优化研究. 计算机系统应用, 2009, 18 (4): 92~95.

第10章

网络可靠性

10.1 引言

近年来,网络技术飞速发展,在众多领域得到广泛应用。如何使用科学的方法定量和定性地理解和研究网络特性,成为网络时代科学研究的一个极具挑战性的课题,被称为“网络新科学(New Science of Networks)”。在现代社会,网络在人们的工作、生活、生产过程中发挥着越来越重要的作用,已成为生活中不可或缺的一部分。生活照明、工业生产离不开电力网络,出行依赖于交通网络,人与人之间的交流通信需要通信网络,信息搜索、查找离不开计算机网络。网络给人类带来极大的便利,大大提高了生产效率和生活质量。但是,一旦网络出现故障,则可能会造成重大影响,甚至是灾难性的事故。例如,2003年美国部分地区电网故障造成大面积停电,严重影响了当地居民的生产生活;2006年中国台湾地区地震导致海底电缆损坏,造成亚洲地区与美国网络通信中断长达20多天;2007年北京奥运售票网站瘫痪,使得相关部门不得不改变门票销售方式;2008年我国南方遭受罕见雪灾,造成90个县市电力中断、7座机场关闭、多段高速封闭、部分火车晚点甚至停运;2008年四川汶川8.0级地震造成通信、交通及物资供应的中断,一时间许多县、乡、村成为事实上的“孤岛”。大量的事实说明,网络可靠性是其效能正常发挥的关键。

可靠性工程技术历经60多年的发展历程,日臻成熟,且不断向综合化、智能化、自动化和全寿命、全过程、全特性的综合方向发展。但现有的研究和实践,大多针对一般的软硬件系统,缺乏对网络可靠性的深入研究。由于网络具有复杂性、动态性、多态性等特点,传统的一般系统可靠性研究成果,如可靠性参数体系、可靠性建模、分析设计、试验评价方法等大多对网络并不适用。因此,以网络为对象开展可靠性研究,形成一套适用于网络的可靠性参数体系、可靠性工程方法,具有非常重要的意义。

网络技术也是现代各国军事和信息竞争的焦点,是未来信息化条件下富国强军的关键。1969年美国国防部最早建立计算机网络,随后,日本、欧洲等也分别建立

了资源共享的计算机网络，逐渐形成国际化的互联网（因特网）。20 世纪 90 年代，因特网扩大到世界范围，创造了人类崭新的互联网军事、经济、文化和科技等新领域。21 世纪是互联网和信息时代，互联网的发展正在带动计算机、微电子、通信和软件等信息产业的发展，成为 21 世纪全球军事和经济的主要推动力。正是这些需求推动因特网向宽带、高速发展，积极探索以光互联网、量子互联网等为代表的下一代的互联网技术迅速发展。大力发展现代网络技术，探索未来网络新技术是现代国防和经济持续发展的双重需求，因此，研究和提高网络可靠性，将对全球经济和军事发展产生深远的影响，具有巨大的应用潜力。网络可靠性的相关理论和方法可为蓬勃发展的网络工程建设提供理论指引和技术手段。

10.2 网络理论的发展历程和相关概念

10.2.1 网络理论的发展历程

回顾网络理论的发展历史，可以看出以图论和拓扑学为代表的应用数学的发展极大地推动了网络理论的发展。多位杰出数学家也各自独立地建立和研究过图论，为网络理论的发展做出了重要贡献。1736 年，欧拉首次在论著中明确提出图论，他所考虑的问题具有很强的实际背景。

图论起源于著名的哥尼斯堡七桥问题。该问题讲述的是 18 世纪发生在东普鲁士的首都哥尼斯堡，也就是现在的俄罗斯加里宁格勒市的事。当时有一条河横贯该城市，在这条河上建有 7 座桥，将河中间的两座岛和河岸连接起来。人们在闲暇时经常在这上边散步，有人提出：能不能每座桥都只走一遍，最后又回到原来的位置。这个看起来很简单却很有趣的问题吸引了大家，很多人在尝试各种各样的走法，然而无数次的尝试都没有成功。谁也没有做到，看来要得到一个明确、理想的答案决非那么容易。1736 年，有人带着这个问题找到了当时的大数学家欧拉，欧拉经过一番思考，很快就用一种独特的方法给出了答案。

欧拉首先把这个问题简化，他把两座小岛和河的两岸分别看成 4 个点，而把 7 座桥看成这 4 个点之间的连线，如图 10-1 所示。图中，A、B、C 和 D 表示陆地，它们之间的连线（弧）表示这 7 座桥。问题是要从这 4 块陆地中的任何一块开始，通过每一座桥正好一次，再回到起点。欧拉在 1736 年解决了这个问题，他用抽象分析法将这个问题简化为第一个图论问题，即把每一块陆地用一个点来代替，将每一座桥用连接两个点的一条线来代替，从而相当于得到一张图。这个问题就简化成能不能用一笔就把这个图形画出来。经过进一步的分析，欧拉得出结论：不可能每座桥都走一遍，最后回到原来的位置。欧拉证明了这个问题没有解，并且推广了这个问题，给出了对

于一个给定的图可以某种方式走遍的判定法则。欧拉图的研究开创了图论这门新的数学分支。这是第一代科学家对网络的开创性贡献，这项工作也使欧拉成为图论及拓扑学的创始人，被誉为图论之父。除了哥尼斯堡七桥问题之外，多面体的欧拉定理、四色问题等也是拓扑学发展史上的著名问题，限于篇幅，在此不再赘述。

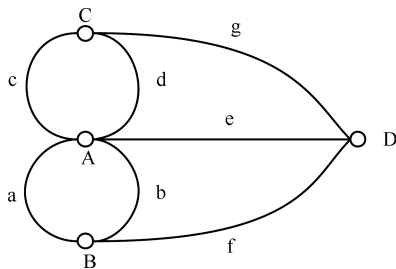


图 10-1 哥尼斯堡七桥问题示意图

对图论（网络科学理论）做出具有里程碑贡献的还有著名的匈牙利数学家 Edös 和 Renyi，他们在 20 世纪 50 年代末到 60 年代建立了著名的随机图理论，用相对简单的随机图来描述网络，形成的理论被称为 ER 随机图理论。在研究过程中一个重要发现就是：在 ER 随机图中随着网络规模的增大，会突然涌现许多重要特性。他们创立的 ER 随机图理论、图论的阈函数和巨大分支涌现的相变等为网络的研究提供了重要的数学理论基础，他们还与一些知名的理论物理学家和数学家，如爱因斯坦、哥德尔、奥本海默等有密切的学术交往。用图论的语言和符号可以精确简洁地描述各种网络，图论不仅为数学家和物理学家提供了描述网络的共同语言和研究平台，而且图论的许多研究方法技巧，能够自然地应用到现在复杂网络的研究中去，成为网络科学研究的有效方法之一。

1998 年，网络的研究又迎来了一次突破性进展，美国康奈尔大学理论和应用力学的博士生 Watts 及其导师 Strogatz 在《Nature（自然）》杂志上发表标题为“Collective Dynamics of ‘small-world’ networks（小世界网络共有的动力学特性）”的论文，提出了小世界网络模型，将同时具有小的平均路径长度和大的聚群系数的特性称为小世界特性。这实际上是 20 世纪 60 年代美国哈佛大学的心理学家 Milgram 提出的著名的小世界实验的一种拓展，是对 Milgram 提出的“六度分离”社会调查后的推断。六度分离的原意是指在美国大多数人中，任意两个人平均最多通过 6 个人就能够彼此认识。

1999 年美国圣母（Notre Dame）大学物理系的 Barabási 教授及其博士生 Albert 在《Science（科学）》杂志上发表了标题为《随机网络中标度的涌现》的文章，提出了一种无标度网络模型，发现了复杂网络的无标度性质（scale free property），并和 M. Newmann、D. J. Watts 共同编辑了“The Structure and Dynamics（结构与动力

学特性)”专著，该书于 2003 年出版，在国际上产生了广泛的影响，引起学术界的高度重视。

网络的小世界特性和无标度特性的发现，以及随后对许多实际网络的研究结果表明，真实世界网络既不是规则网络，也不是随机网络，而是兼具小世界和无标度特性，其统计特性不同于规则网络和随机图。这在全世界学术界激起了千层浪，围绕着复杂网络的相关研究的文章层出不穷，网络科学的综述和专著不断涌现，从物理学到生物学，从社会科学到技术网络，从工程技术到经济管理等众多领域，吸引了越来越多人的注意，引起了各领域人员的高度重视，推动了相关技术的飞速发展。

10.2.2 网络的概念和特征量

为了全面刻画复杂网络的性质、表示复杂网络的拓扑结构特性，对复杂网络的动力学特性进行研究，相关研究人员提出了有关复杂网络的一系列基本概念、特征量和度量方法。图 10-2 给出了网络的基本概念和主要特征量，包括：节点度分布、强度分布、边权分布、平均路径长度、群聚系数，这些是重要的特征量。另外，网络还有其他特征量，如介数及其分布、最大连通分支的规模分布、度-度关联性（相称性系数）、群聚度关联性、模块性等。

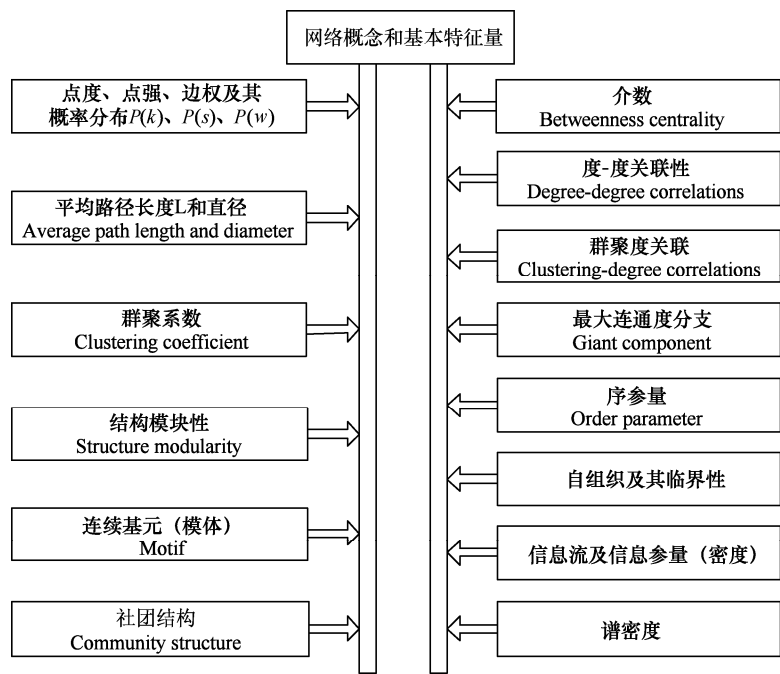


图 10-2 网络的基本概念和特征量

1. 节点度分布、强度分布和边权分布

节点度分布、强度分布和边权分布是反映网络拓扑特性的重要特征量。度 (Degree) 也称为连通度, 节点的度指的是与该节点连接的边的条数。度在不同的网络中所代表的含义不尽相同, 例如, 在城市航空交通网中, 度分布表示城市之间的航线多少和重要程度, 度越大的城市, 其重要性就越大; 在社会网络中, 度可表示个体的作用力和影响程度, 一般情况下, 一个节点的度越大, 表示其在整个网络系统组织中的作用和影响就越大, 反之亦然。度分布则表示节点度的概率分布函数 $P(k)$, 它是节点有 k 条边连接的概率。

在有权网中, 与节点度 k_i 相对应的自然推广就是点强度或点权 (Vertex Wight), 用 s_i 表示。其定义为: $s_i = \sum_{j \in N_i} w_{ij}$, 其中 N_i 是节点 i 的近邻集合, w_{ij} 是节点 i 和节点 j 之间的边的权重值, 如果值为 0, 表示两个节点之间没有连接。点强度分布 $P(s)$ 与度分布 $P(k)$ 的作用类似, 主要是考察节点具有点强度 s 的概率, 这两个分布结合在一起, 提供了有权网络的基本统计信息。点强度既考虑了节点的近邻数, 又考虑了该节点和近邻之间的权重, 是该节点局域信息的综合体现。当边权与网络的拓扑结构无关时, 点强度与度的函数关系为 $s(k) \approx \langle w \rangle k$, 其中 $\langle w \rangle$ 为边权的平均值。当边权与拓扑结构具有相关性时, 点强度与度的函数关系一般为 $s(k) \approx Ak^\beta$, $\beta=1$ 但 $A \neq \langle w \rangle$, 或 $\beta \neq 1$ 。

2. 平均路径长度

网络中拓扑特性的另一个重要的特征度量是平均路径长度 (Average Path Length, APL), 它是网络中所有节点对之间的最短距离平均值。这里节点间的最短距离是指从一节点到另一节点所要经历的边的最小数目, 其中所有节点对之间的最大距离称为网络的直径 (Diameter)。平均路径长度和直径衡量的是网络的传输性能与效率。平均路径长度 APL 的计算公式为:

$$APL = l = \frac{1}{N(N-1)} \sum_{i \neq j \in V} d_{ij} \quad (10-1)$$

式中 d_{ij} 为节点 i 和 j 之间的最短距离。

对于非连通图, 可能存在 $d_{ij} = \infty$, 则根据上式计算得出 $l = \infty$ 。为了避免这一问题, 通常定义网络的平均最短路径长度的值为所有存在路径相连的节点对之间的平均最短路径长度, 或者定义 l 为所有节点对之间的调和平均最短路径长度, 即:

$$l^{-1} = \frac{1}{N(N-1)/2} \sum_{i > j} d_{ij}^{-1} \quad (10-2)$$

考虑与每条边关联的物理距离是有关网络分析的重要问题。对于位于 D 维欧氏空间中的网络, 直接相连的两点间的长度可以看成两点间的欧氏距离, 但对于一般

的有权网络并没有明确的距离概念，每条边上的距离可以看成是权重的某种函数。此时，就必须注意权重是相异权还是相似权。对于相异权，可以直接定义两个相连节点之间的距离 $l_{ij} = w_{ij}$ ，而对于相似权，则可令 $l_{ij} = 1/w_{ij}$ ，当然也可采用其他形式把相似权转化为距离。

其中，更为关键的问题是如何计算没有直接相连的节点之间的距离。在无权网中，经过边数最少的路径即为两点间的最短路径，但是在有权网中由于每条边权重值的差异，网络中的距离通常不再满足三角不等式，从而导致经过边数少的路径不一定为两点间的最短路径。假设节点 i 和节点 k 通过两条权重分别为 w_{ij} 和 w_{jk} 边相连，对于相异权，节点 i 和 k 之间的距离可以直接取和： $l_{ik} = w_{ij} + w_{jk}$ ，而对于相似权，节点 i 和 k 之间的距离就必须使用调和平均值： $l_{ik} = w_{ij} w_{jk} / (w_{ij} + w_{jk})$ 。以此为基础，就可以获得任意连续路径的距离值，进而可以得到有权网络中任意两点间的最短距离以及网络的平均最短距离。而其他网络的全局统计量，比如效率（efficiency）、介数（betweenness）等，就可以在考虑有权最短路径的基础上进行计算。

3. 群聚系数

群聚系数（Clustering Coefficient）用来衡量一个复杂网络的集团化程度，它是表征网络性质的另一个重要特征参数。该概念有其深刻的社会根源。对社会网络而言，集团化形态是一个重要特征，集团表示网络中的朋友圈或熟人圈凝聚力的程度，集团中的成员往往相互熟悉，群聚系数就是刻画这种群集现象的集团化属性。

设网络中节点 i 有 k_i 条边，将它与其他节点相连，这 k_i 个节点就称为节点 i 的邻居。这 k_i 个节点最多有 $k_i(k_i - 1)/2$ 条边。设 k_i 个节点之间实际存在的边数为 E_i ，那么可以定义聚类系数为 E_i 与 $k_i(k_i - 1)/2$ 之比，即：

$$C_i = \frac{E_i}{k_i(k_i - 1)/2} \quad (10-3)$$

对于度为 0 或者 1 的节点 i （节点没有邻居节点或者只有 1 个邻居节点），令 $C_i = 0$ ，整个网络的聚类系数 C 就是所有节点 i 的聚类系数 C_i 的平均值，即：

$$C = \frac{1}{N} \sum_{i=1}^N C_i$$

从几何特征上，式（10-3）还可以定义为：

$$C_i = \frac{\text{与节点 } i \text{ 相连的三角形的数目}}{\text{与节点 } i \text{ 相连的三元组的数目}} \quad (10-4)$$

平均网络的群聚系数 C 为所有节点群聚系数的算术平均值，即 $C = \frac{1}{N} \sum_{i=1}^N C_i$ ，

其中 N 为网络的阶（规模大小）。不仅是社会网络，在其他类型的网络中，都普遍

存在群聚现象。例如,已经发现的小世界效应特性,具有大的群聚系数和小的平均最短路径长度。节点的群聚系数反映该节点的一级近邻之间的集团性质,近邻之间的联系越紧密,该节点的群聚系数越高。

4. 介数

介数是一个全局变量,反映节点或边的作用和影响力,可分为节点介数和边介数两种。如果一对节点间共有 B 条不同的最短路径,其中有 b 条经过节点 i ,那么节点 i 对这对节点的介数的贡献为 b/B 。把节点 i 对所有节点对的贡献累加起来再除以节点对总数,就可得到节点 i 的介数。通常可以用来刻画一个网络的中心化程度,用 $B_{(x)}$ 表示节点 x 的介数,则可表示如下:

$$B_{(x)} = \frac{1}{M} \sum_{i \neq j} \frac{g_{ij}(x)}{g_{ij}} \quad (10-5)$$

其中 $g_{ij}(x)$ 为在节点 i 和节点 j 之间的最短路径中包含有节点 x 的最短路径长度;
 g_{ij} 为在节点 i 和节点 j 之间所有的最短路径条数; M 为网络中的节点对总数。

边的介数定义为所有节点对的最短路径中经过该边的数量比例。研究表明,节点的介数与度之间存在很强的相关性,不同类型的网络,其介数分布也大不一样。

10.2.3 网络的分类

目前国际上对于网络还缺乏明确而统一的分类,根据目前有关文献的提法和我们的观点,对网络可进行简单的分类,如图 10-3 所示。

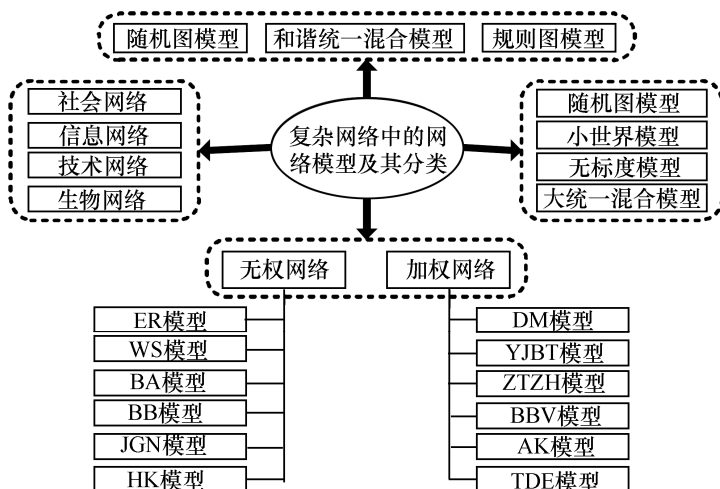


图 10-3 网络类型和模型分类示意图



1. 按系统内涵分类

根据 Newman 的观点, 现实网络大致分为 4 大类: 社会网络、信息网络、技术网络和生物网络。这 4 种网络, 虽然它们的网络结构形式各不相同, 彼此描述的系统内涵各异, 其节点和边的定义差别也很大, 但它们却具有一些相同的特征: 网络节点间的作用很复杂, 而且高度不规则; 在度和群聚系数等网络特征度量方面, 节点之间的差异性非常大, 表现出不对称性。尽管这些网络大而复杂, 但是节点间的平均最短路径长度却很小, 呈现出小世界特性。大量的实证研究表明: 现实世界中的许多网络具有下面三个共同特性: 节点度服从幂律分布, 群聚系数高, 节点间的平均路径长度小。我们认为, 根据不同领域的网络, 除了上述网络大致划分外, 还视具体领域不同网络类型而异, 例如应有物理网络、生态网络、军事网络、经济网络、通信网络、交通网络、工程网络等等。每类又有不同的网络, 例如生物网络具有: 神经网络、新陈代谢网、蛋白质网络等。

2. 按权值分类

根据网络的边有无权值, 将网络分为有(加)权网络和无权网络。目前大多数研究集中在无权网络上, BA 无标度网络及其各种变种是最具代表性的无权网络, 也属于广义随机网络, 可以反映节点之间简单连接方式和相互作用的最主要信息, 但是不能描述节点之间起着重要作用强度的差异情形, 而有权网络则能够提供更加细致的刻画, 不仅能够反映实际网络的拓扑结构, 而且可以反映真实网络上的动力学特征。因此, 目前有权网络是一个重要研究方向。

3. 按网络生成方法分类

根据生成方法的随机性大小, 我们可将网络分成随机性网络、确定性网络和混合网络。随机网络是按照随机方式生成的, 不过即使生长规则相同, 每次在电脑上模拟随机生成的网络却不尽相同, 存在差异性; 确定性网络是按照确定方式生成的, 优点是其拓扑特性可以精确求解。除了这两种极端方式外, 真实网络应有两者混合生长的方式, 混合方式符合统一世界的基本事实。

从复杂网络的角度来看, 根据网络的生成机制, 可以将网络分为: 规则网络、随机网络、小世界网络和无标度网络。

(1) 规则网络

规则网络是由 N 个节点组成的环状网络, 网络中每个节点只与它最近的 K 个节点连接, 在规则网络中, 每个节点具有相同的度和簇系数。节点的度分布为 δ 函数, 即 $P(k)=\delta(k-K)$, 节点簇系数为 $C = \frac{3(K-2d)}{4(K-d)}$, d 为网络维数, 集聚程度较高, 一维

规则网络的平均路径长度 L 较大, 与节点数呈线性比例关系, 即 $L \propto N/2K$ 。

(2) 随机网络

随机网络理论由匈牙利数学家 Erdős 和 Rényi 提出, 他们提出的模型称为经典的 Erdős-Rényi (ER) 模型, ER 模型的定义为: 在由 N 个顶点、 $C_N^2 = N(N-1)/2$ 条边构成的网络中, 随机连接 g 条边形成一个随机网络, 记为 $G_{N,g}$, 由这样的 N 个节点, g 条边组成的网络共有 $C_{N(N-1)/2}^g$ 种, 构成一个概率空间, 每一个网络出现的概率是相等的。ER 随机图的节点度服从泊松分布, 它具有较小的平均路径长度和较小的簇系数。

(3) 小世界网络

最早的小世界网络模型是 Watts 和 Strogatz 在 1998 年提出的 (WS 模型), 该模型由一个具有 N 个节点的环开始, 环上每一个节点与两侧各有 m 条边相连, 然后对每条边以概率 p 随机进行重连 (自我连接和重边除外), 这些重连的边叫长程连接, 长程连接大大减小了网络的平均路径长度, 而对网络的簇系数影响较小。在 WS 模型提出不久, Newman 和 Watts 对 WS 模型进行了改进, 提出了 WS 模型的一个变体模型, 通过在随机选择的节点对之间增加边作为长程连接, 而原始格上的边保持不动。

(4) 无标度网络

1999 年, Barabási 和 Albert 通过追踪万维网的动态演化过程, 发现了许多复杂网络具有大规模的高度自组织特性, 即多数复杂网络的节点度服从幂律分布, 并把具有幂律度分布的网络称为无标度网络。最原始的无标度网络模型称为 Barabási-Albert (BA) 模型 (或称为 BA 网络), 它是第一个随机的无标度网络模型。在 BA 模型生成的初始时刻, 假定系统中已有少量节点, 在以后的每一个时间间隔中, 新增一个节点, 并与网络中已经存在一定数目的不同节点进行连接。当在网络中选择节点与新增节点连接时, 假设被选择的节点与新节点连接的概率和被选节点的度成正比, 人们将这种连接称为择优连接。BA 模型的平均路径长度很小, 簇系数也很小, 但比同规模随机图的簇系数要大, 不过当网络趋于无穷大时, 这种网络的簇系数均近似为零。

10.3 网络可靠性发展历程及相关概念

10.3.1 网络可靠性研究的历程

网络的可靠性研究经历了一个从简单到复杂的发展过程: 从最初的设备可靠性发展到网络的可靠性, 进而发展到网络的完成性。简单来说, 网络的可靠性研究涉

及抗毁性、生存性、可用性（或有效性）和完成性 4 个方面。

迄今为止，对通信网系统可靠性的研究已有大量的文献发表，它们广泛讨论网络可靠性的定义、测度、设计与综合评价方法，以及提高改善网络可靠性的途径等。

1. 早期的研究

1955 年 C Lee 对电信交换网的研究是当前可追溯的对通信网系统可靠性最早的研究。C Lee 在《Analysis of Switching Networks》一文中，首次提出了以网络连通为规定功能的可靠性指标，将由于网络部件故障导致网络传输容量下降而引起的阻塞定义为链路故障，确立了以“能实现连通功能的概率”为度量的端可靠度参数。1956 年 Moore 和 Shannon 研究提出了两端可靠度这一度量参数，为网络可靠性研究奠定了重要基础。

1969 年世界上第一个计算机网络 ARPANET（美国高级研究计划署网络）在美国诞生之后，网络可靠性引起了各方面的广泛重视，也掀起了通信网系统可靠性研究的第一次热潮。网络可靠性的研究早期是将网络连通作为“规定功能”来进行研究。采用图论、概率论等，将物理通信网抽象为节点和链路，及其相互连接关系构成的有向或无向的图，对节点和（或）链路故障情况下的网络连通性进行研究，主要用网络抗毁性（Invulnerability）和网络生存性（Survivability）这两个网络连通可靠性测度来衡量。

抗毁性是指在拓扑结构完全确定的网络中，在理想的破坏方案作用下，网络能够保持连通的能力。对于一个抽象网络，网络的抗毁性是指至少需要破坏几个节点或几条链路才能中断部分节点之间的联系，即指出破坏一个网络的困难程度。抗毁性指标是确定性的，仅仅和网络的拓扑结构有关，常用的指标有连接度和粘聚度。连接度和粘聚度最初是由 Frank 等提出的。

此外，Wilkov 针对通信网络的通信实际，提出了一种相对实用的网络连通度和粘聚度概念，即对于网络直径为 k 的网络，为使网络直径 k 超过阈值 k_m 时必须去掉的最少节点数或最少边（或弧）数，其中网络直径是指网络中所有两两节点之间最短径长的最大值。Boesch 等提出了具有一般意义的网络连通度和粘聚度概念，该概念是基于割集的，即：为了把一个具有 m 个节点的子网从原网络中分离出来所需去掉的最少链路数或边数。基于割集的连通度和粘聚度概念是比较适合地域通信网的抗毁性分析与评价的指标。

网络的抗毁性只是从图论的角度出发，把具体网络抽象为纯图，在假定节点和链路可靠的前提下，把评估网络的连通度作为可靠性指标。

网络生存性是指对于节点或链路具有一定失效概率的网络在随机性破坏作用下，能够保持网络连通的概率。

生存性是基于概率论和图论的知识提出来的，描述了随机性破坏以及网络拓扑结构对网络可靠性的影响。生存性指标是概率性的，它不仅和网络的拓扑结构有关，也和网络部件的故障概率、外部故障以及维修策略等有关。常用的指标是连通

概率,是指在规定的时间内网络一直保持连通的概率。针对分析的范围不同,其可靠度的意义也有所不同,主要包括端端可靠度、 k 端可靠度和全端可靠度。其中,端端可靠度是人们关心较多的指标。

端端可靠度是指网络中任意两个节点之间存在一条连通路径的概率。现在的许多文献都是针对端端可靠度进行研究的。从网络节点故障与否的角度,该指标大体可分为两类:节点可靠与节点具有一定生存概率的情况。针对每一类指标,都出现了许多手工或计算机化的计算方法。另外,Varshney 等提出了一个链路容量可变通信网络的复合性能指标:源终点成功性,它指出了能传输一定容量信息的端端连接概率,其实质也是端端可靠度。

k 端可靠度是指网络保持 k 个端点之间连通的概率,即网络中任意两个给定的节点子集 k 中各节点均处于工作状态,且各节点之间至少存在一条路径的概率。该指标的计算比较困难,解析方法只能解决比较简单的网络 k 端可靠度问题,对这一问题的计算有较深入的研究。

全端可靠度是衡量整个网络在部件故障情况下的生存能力。Gilbert 和 Kelmans 提出了全端可靠度概念原型,其假设节点绝对可靠,链路具有相同的生存概率。Frank 把它推广为节点和链路具有一定生存概率的情况。Srivaree-Ratana 等把神经网络方法运用到全端可靠度的计算中,得到其近似解。Sawionek 等假定节点完全可靠,链路故障统计独立,然后用离散近似优化技术求得网络的全端可靠度。

另外,Baran 根据部件的生存概率利用 Monte Carlo 法模拟对网络的随机破坏,从剩余子网中选择较大的连通子网络,用该子网络的节点数占原网络节点数的比率作为网络的连通概率,这一指标在通信网可靠性的设计与评价中有重要意义。

2. 第二阶段的研究

20 世纪 80 年代前后,通信技术快速发展,特别是动态路由技术引入之后,人们逐步意识到通信网连通性只是通信网正常运行的必要条件,网络容量和时延等影响电信业务完成的因素也应在网络可靠性研究中予以考虑。第一阶段的网络可靠性研究主要考虑网络部件失效使得网络拓扑结构变化,从而对网络连通可靠性产生影响。随着研究的深入,第二阶段的网络可靠性研究重点逐步转向由于网络部件容量、网络传输时延,或网络路由策略等影响因素下的网络使用可靠性参数的选择和计算优化上,网络可用性(Availability,又称有效性)和网络完成性(Performability)是这个阶段研究的主要内容。

网络的可用性是描述网络在外部资源可用的条件下,在规定时间内任何时刻,能执行所需功能的能力。该指标可以从两个方向加以理解:其一是针对构成网络的设备提出的,它不仅反映了设备的可靠性,还与其维修性、保障性有关;其二是指在部分设备故障的条件下,网络能执行所需功能的能力。把可用性作为网络的

可靠性指标表现在设备的可靠件及其对网络整体的影响上。

网络的完成性描述网络在部件故障条件下,满足通信业务性能要求的程度,这是基于网络业务性能的可靠性测度。完成性包括网络的吞吐量、传输时延等。

较早提出完成性指标的是 Barberis 等给出的加权端端连通概率,该指标把网络的端端信息流量对相应的端端连通概率加权,并求全网的平均值,该指标可用于比较具有不同拓扑结构和不同流量分布的通信网可靠性,但没有涉及网络的具体业务性能。为此,Barberis 等还提出了网络的另一种完成性指标——网络的吞吐量超过一个给定阈值的概率。Deuermeyer 提出了一种基于网络吞吐量的完成性指标。此外,传输时延也是一种重要的完成性指标,它主要取决于信息在中继节点的排队时间和处理时间。Park 等在其论文中曾采用了这一指标,Bonaventura 针对线路交换网和报文交换网分别提出了基于时延的完成性指标,反映了用户对网络时延的要求。Kyandoghere 等研究了网络故障后路由策略对网络的影响问题,提出了网络完成性指标框架。应该说,网络的完成性研究更面向业务性能,面对网络用户,也反映了网络的服务性能,是地域通信网可靠性测度的较高层次。

3. 第三阶段的研究

20 世纪 90 年代后,随着认识的深入,网络可靠性的研究对象从单纯的通信网络研究拓展到电力网、交通运输网、遥控遥测网等各个领域。在这个阶段中人们针对真实网络的实际情况提出了不同的网络拓扑结构模型,引发了新一轮网络可靠性研究热潮。

1998 年 Watts 等人为了体现真实网络中高聚类和小平均路径长度的特点,提出了小世界 (Small World, SW) 网络模型并定义了 SW 图。1999 年 Barrsbási 等人为了体现真实网络中连接度分布呈幂律分布的特性,又提出了无标度 (Scale-Free, SF) 网络模型并定义了 SF 图。通过众多的研究证实:大规模人造网络系统大多具有小世界效应 (Small World Effect) 和无标度特性 (Scale Free Property),网络的拓扑结构与网络的健壮性、可靠性以及脆弱性之间存在着一定的相关关系。

1995 年芝加哥大学的 Michael Suk-Young Chwe 提出通信网战略可靠性的概念,利用对策论分析如何选择通信网。

1999 年 Chat Srivaree-ratana 和 Alice.E.Smith 利用人工神经网络 (ANN) 估计全端网络可靠度,提出一种称为 ANN 预测模型的方法。

吕久明等对军事通信网抗毁性能的神经网络方法进行了研究,提出综合考虑可靠性和延时性能的代价函数,借助自组织竞争 ANN 对其进行分析与仿真。

李德毅等以模糊可靠性和隶属云思想为基础,建立了系统的能力雷达图模型,通过半实物模拟对可靠性、抗毁性和抗干扰性进行统一评测。

张勇等利用云模型建立了军事短波通信系统的仿真模型,给出了抗干扰性能仿真评估的指标,对仿真结果采用云模型及不确定性推理进行评估。

樊鹤红等对光网络模糊可靠性评估模型进行了研究,将网络看成是具有多个工作状态的复杂对象,在定义了网络功能的量化参数功能值的基础上,阐述了定量描述和定性描述之间的关系,定义了多工作状态对象的可靠性与可用性,并给出了多工作状态网络的模糊可靠性评估模型的算法和步骤。

工业和信息化部电子第五研究所、北京航空航天大学等单位近年来对通信网络可靠性指标体系、可靠性建模、分析设计和仿真方法等进行了较为深入的研究,取得了系列成果,并在大型军事和民用通信网络的可靠性工程实践中取得应用成效。

工业和信息化部电子第五研究所研发了网络可靠性方面的软件工具——“通信网络业务质量与可靠性分析软件 CNQRAS”。CNQRAS 是通信网络业务质量 (QoS) 与可靠性分析专业软件,具有:设备、拓扑、业务和故障建模;QoS 统计分析、可靠性、抗毁性、可用性、完成性分析;网络设计方案优选;网络设计优化;网络最坏情况分析等功能,运用解析建模、仿真模拟、统计分析等手段,获取网络性能、QoS 和可靠性参数,可用于电信网和军事通信网等的 QoS,以及可靠性指标论证、分析设计优化及虚拟验证。

10.3.2 网络及可靠性的相关术语

有关网络及可靠性术语的定义如下。

1. 网元 (network element)

网元是指网络功能部件或子系统。

2. 网络业务 (network service)

网络业务是指提供给网络用户的网络业务功能。

3. 服务质量 (quality of service)

服务质量是指综合的业务性能,表征用户对业务的满意程度。

4. 网络故障 (network failure)

网络故障是指由功能故障、自然灾害或人为引起的灾害导致的一个或多个网元部分或全部故障。

5. 粘聚度 (cohesion)

粘聚度是指断开网络中一对节点之间的所有通路所需去掉的最少链路数。

6. 连通度 (connectivity)

连通度是指断开网络中一对节点之间的所有通路所需去掉的最少节点数。

7. 业务损失率 (loss of service)

业务损失率是指网络在节点（或链路）被毁后，其剩余的业务量与原有业务量之比。

8. 全功能可用度 (availability of all functions)

全功能可用度是指在网络规定的功能中，全部功能正常运行的时间与总任务时间（或试验时间）之比。

9. 主要功能可用度 (availability of key functions)

主要功能可用度是指在网络规定的功能中，主要功能正常运行的时间与总任务时间（或试验时间）之比。

10. 最低功能可用度 (availability of minimum function)

最低功能可用度是指在网络规定的功能中，最低功能正常运行的时间与总任务时间（或试验时间）之比。

11. 业务保障性能 (service support performance)

业务保障性能是指网络运营商提供业务并且在使用过程中提供帮助的能力。

12. 业务运行性能 (service operability performance)

业务运行性能是指网络保证业务能够支持用户成功而且方便地操作的能力。

13. 服务能力性能 (service ability performance)

服务能力性能是指网络保证在用户请求提供业务和在请求过程中继续提供服务的能力。服务能力性能包括业务接入能力性能和业务保持能力性能。服务能力表示在业务建立、保持和释放过程中的网络响应能力。

14. 业务完整性 (service integrity)

业务完整性是指网络保证业务建立之后传输损伤不超过限定范围的能力。

10.3.3 网络可靠性定义

根据网络的特点和功能，我们可以将网络可靠性定义为：网络在规定条件下和规定时间内，完成其规定连通和流通功能的能力。

规定条件包括网络使用时的环境条件和工作条件。环境条件通常是指网络所在的空间，对网络工作状态有影响的物理、化学、生物以及其随时间的变化规律，其

中涉及的主要因素包括温度、湿度、振动、冲击、辐射等。环境条件的不同,将直接影响到网络中各种硬件的可靠性水平。工作条件包括网络使用时的应力条件、维护方法、使用时对操作人员的技术等级要求等。工作条件的不同,除影响到网络中硬件、软件的可靠性外,还对网络结构、运行机制的可靠性有所影响。

规定时间是指网络规定的任务时间。随着网络任务时间的增加,网络出现故障的概率将增加,而网络的可靠性将是下降的,因此,谈论网络的可靠性离不开规定的任务时间。一般地,网络的规定时间可以日历时间计,也可以工作时间计。

规定连通和流通功能是指网络规定了必须具备的连通、流通功能的技术指标。所要求网络功能的技术指标的高低,直接影响到了网络可靠性指标的高低。例如,要求网络80%的节点能满足连通、流通功能要求与要求90%的节点满足同样要求,所得出的可靠性指标是大不一样的,因此,在分析评价网络的可靠性时,必须首先明确要求网络完成的连通和流通功能是什么,其技术指标要求是什么,才能给出明确的网络故障判据。

10.3.4 网络故障的来源

网络一般由若干不同的子网络构成。引起网络失效的原因多种多样,只有明确网络的故障来源,才能准确地理解网络故障的特性,最终找出控制网络故障的有效措施。李瑞莹等人以计算机网络为例,统计48起计算机网络故障的故障模式、故障原因及故障影响。统计分析表明,故障类型包括:断路、瞬时断路、时延、丢包和错误,其中断路故障的所占比重最大,为54%,如图10-4(a)所示。造成这些故障的各个原因的比例如图10-4(b)所示,其中硬件和软件所占比例较大。

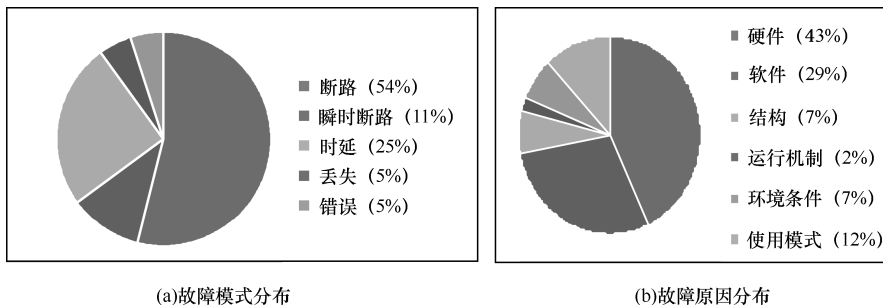


图 10-4 网络故障模式和故障原因分布

10.3.5 网络故障的分类

网络故障的分类可以按多种方式进行,例如,按故障原因、产品层次、故障程度、主从关系等进行分类。



1. 按故障原因分类

网络故障的形成原因可以将网络故障分成两类：过应力型故障和耗损型故障。

- 过应力型故障是网络长时间暴露在应力大于正常工作强度的环境中造成的网络故障。与普通系统相比，网络系统的应力除了来源于网络组件受到的力学、电学等各类关系作用外，还可能来源于流量负荷-容量关系的作用，所以应力分析也相对较难。
- 耗损型故障是网络长时间在一定应力条件下造成的，损坏是不断累积起来的，不同于普通的系统，除了有机械耗损、电子耗损、化学耗损，还会有传输耗损。

2. 按产品层次分类

根据故障发生的产品层次可以将网络故障分为节点硬件故障、节点性能下降型故障、设备级故障、应用层软故障和网络级故障。

- 节点硬件故障：由于硬件原因使得节点之间无法进行通信的故障。
- 节点性能下降型故障：节点自身性能参数值超出正常范围，例如 CPU 利用率高、内存可用率低、电池电量低等。
- 设备级故障：网络中某些特定设备出现的故障，如 GPS、摄像头等设备故障。
- 应用层软故障：某些重要的服务程序（如监控程序，E-mail 服务程序等）未正常运行的网络故障。
- 网络级故障包括节点行为异常（如节点长时间持续发送广播或大量数据的异常行为），以及网络状态异常（如平均丢包率，网络平均传输延迟等参数值超出正常范围）、其他可以影响整个网络通信质量的故障。

3. 按故障程度分类

根据网络故障引发的网络性能的衰退程度可以将网络故障分为硬故障和软故障。

- 硬故障：由于网络硬件设备引起的，可使网络吞吐量、传输量减少到零的故障。
- 软故障：故障发生时，网络仍能够提供服务，但网络性能下降，如带宽损失、延时增大等情况。

4. 按主从关系分类

根据故障发生的主从关系可以将故障分为源故障和级联故障。

- 源故障：由于网络节点、设备本身硬件设备的问题不能工作或是处理能力不足，而使网络性能下降，不能满足服务要求造成的故障称为源故障。
- 级联故障：由于其他节点故障，引起网络中负载重新分配，导致当前节点发生故障，或是由于某一个或某些节点故障导致网络中依赖于他们的节点发生故障，我们称这种故障为级联故障。

10.4 网络可靠性研究的理论方法

网络科学由于其广泛交叉性和复杂性，涉及众多学科的知识 and 理论基础，特别是数学、统计物理学、计算机与信息科学等。图 10-5 给出复杂网络涉及的相关理论方法，主要包括：图论、统计力学、凝聚态物理、非线性科学、复杂性科学、数值计算方法、系统科学和现代控制理论等。而上述每学科还包含更详细的基础知识，如数学涉及随机图理论、概率论与随机过程分析、马尔可夫过程与马尔可夫链方法、随机微分方程解法、组合分析方法、拓扑学、优化理论、常微分和偏微分方程解法等。

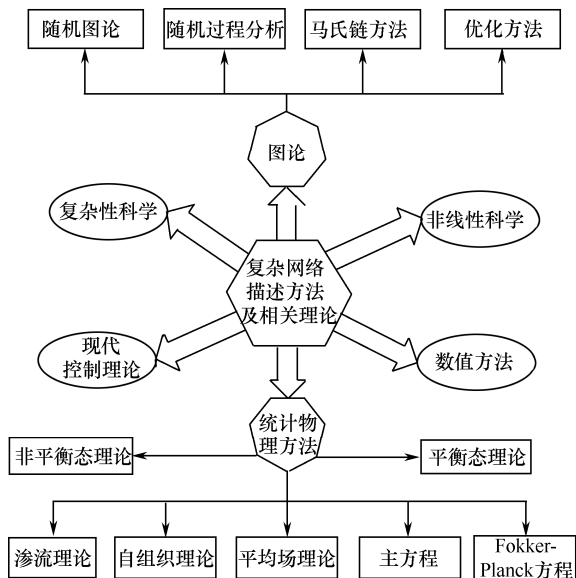


图 10-5 网络可靠性研究的理论方法

统计物理学或统计力学是用概率统计的方法，对由大量粒子（或元素）组成的宏观物体的物理性质及宏观规律进行微观解释的理论物理学分支，它架起了从微观到宏观研究的桥梁，不仅为各种宏观复杂系统（气体、液体、固体、等离子体等）提供理论依据，而且现在为新生成的网络科学提供了理论基础和有力工具，发挥着重要的作用。

10.5 网络可靠性度量参数体系

10.5.1 建立原则

网络可靠性度量参数体系的建立，应遵循以下原则。

1. 系统性

网络可靠性参数体系要综合全面地反映网络可靠性的各个方面，参数体系内的各类参数相互联系，形成一个完整的参数体系系统。

2. 科学性

网络可靠性参数体系要建立在科学、客观的基础上，参数必须概念清晰、明确，具有具体的科学内涵、明确的物理意义、标准的测算方法、规范的统计计算方法等。

3. 必要性

网络可靠性参数体系中的参数具有代表性，应该是必不可少的，不能出现冗余，且参数的内容简单明了与准确。

4. 完备性

网络可靠性参数的体系覆盖面广，能全面并综合地反映体现影响网络可靠性的所有因素。

5. 可行性

网络可靠性参数体系中的参数必须简单实用，易于获取，即在度量技术、投资和时间上是可行的，可用准确可信的方法和合适的仪器进行监测。

6. 协调性

参数间可能存在相关性，网络可靠性参数体系中的参数应当协调一致。

10.5.2 网络可靠性的通用参数体系

不同的网络对象对应的参数体系具有很大的差异，但是从总体上来说，根据以上所提的参数体系的六条建立原则，构建的网络可靠性参数体系要能够同时反映下述几个方面。

1. 不同功能要求

如前所述，网络可靠性的定义包括了两项功能：连通和流通。流通功能又包含了及时传输、完整传输以及正确传输的含义。因此，为了同时反映网络不同功能要求的可靠性，可将网络可靠性参数划分为连通可靠性、流通可靠性两类。其中，连通可靠性关注的是网络的功能层次，判断网络能否实现对应的功能；流通可靠性关注的是网络性能，判断网络实现对应功能的好与坏，流通可靠性又划分为及时可靠性、完整可靠性以及正确可靠性三类。

2. 不同度量范围

对于网络整体的可靠性水平，可用 k/N 端的可靠性进行度量，考察网络中 k 个终端间的可靠性水平。这 k 个终端包含在一个端点子集 N 中 ($N \subseteq V$, V 是网络中所有端点的集合; $2 \leq k \leq n$, n 是端点子集 N 的端点数)，通过对端点子集 N 的选择可以反映网络中不同优先级、不同区域、不同层次端点间的可靠性水平。

对于网络群体的可靠性水平，可用 $M-k/N$ 端的可靠性度量，反映网络端点子集 M ($M \subset V$) 对网络可靠性的群体感知，是端点子集 M 中 m 个端点的个体可靠性参数的函数 (m 是端点子集 M 的端点数)。

对于网络个体可靠性水平，可用 $1-k/N$ 端的可靠性进行度量，反映单个网络端点对网络可靠性的个别感知。其中，考察的一端是网络中某个固定的端点 s ，考察的另一端则是网络中的 k 个端点，这 k 个终端是包含在一个端点子集 N 中 ($N \subset V$, 且 $s \notin N$)。

3. 不同度量角度

在网络可靠性参数中应既有概率维参数，又有时间维参数。为了度量网络任务可靠性水平，可将网络可靠性参数划分为包括任务可靠度和平均严重故障间隔时间两类。

同时考虑网络的不同功能要求（连通、流通）、不同度量范围（整体、群体、个体）、不同度量侧面（任务可靠度、平均严重故障间隔时间），则构成了网络可靠性的三维参数体系，如图 10-6 所示。

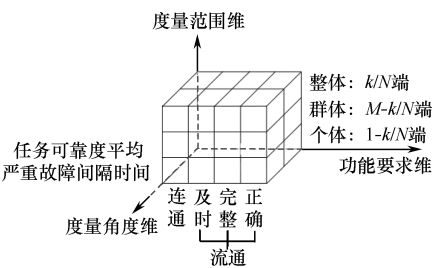


图 10-6 网络可靠性的三维参数体系

总结下来，网络可靠性的度量参数如图 10-7 所示。

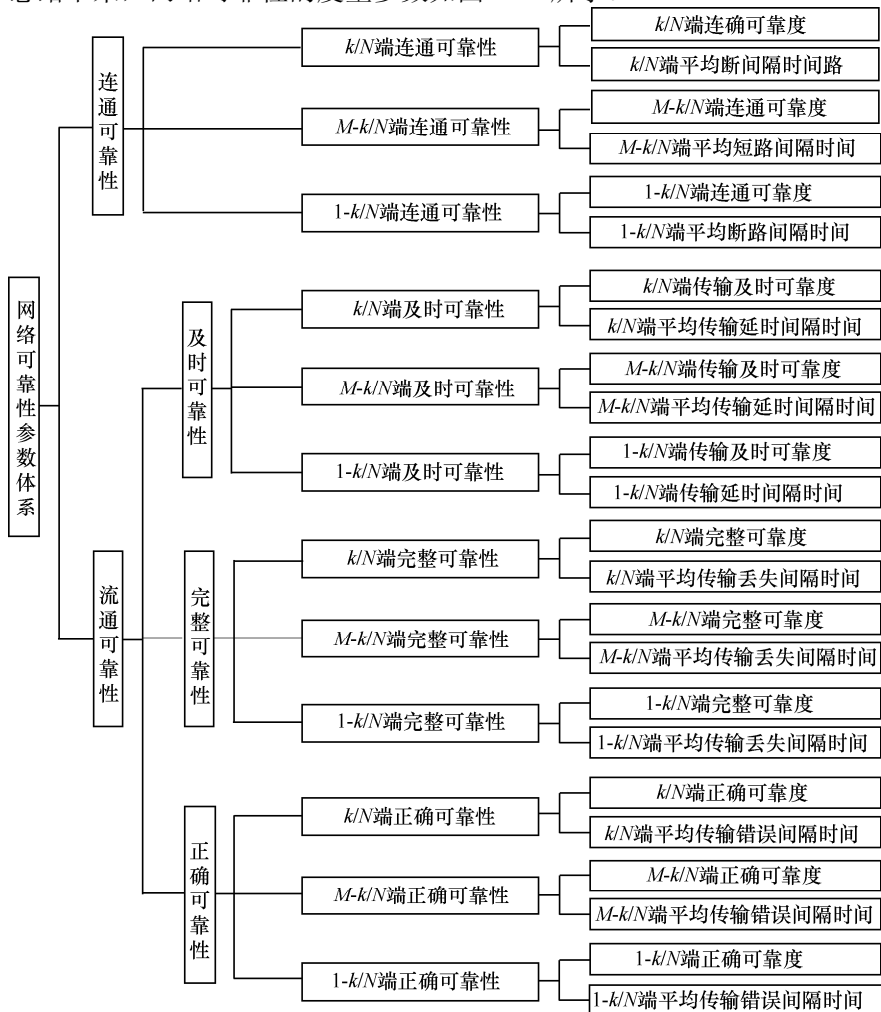


图 10-7 网络可靠性度量参数

10.5.3 通信网络可信性参数体系

在不同的实际网络可靠性研究中考察的方面可能不一致，以通信网络为例，主要考察的是通信能否完成、完成的程度（数据包丢失数量、误码多少和时间延迟长短等），从五性的角度对通信网络的可信性参数体系进行研究，可以分为综合参数、完成性参数、抗毁性参数、可靠性参数、维修性参数、保障性参数、恢复性参数和安全参数，如图 10-8 所示。

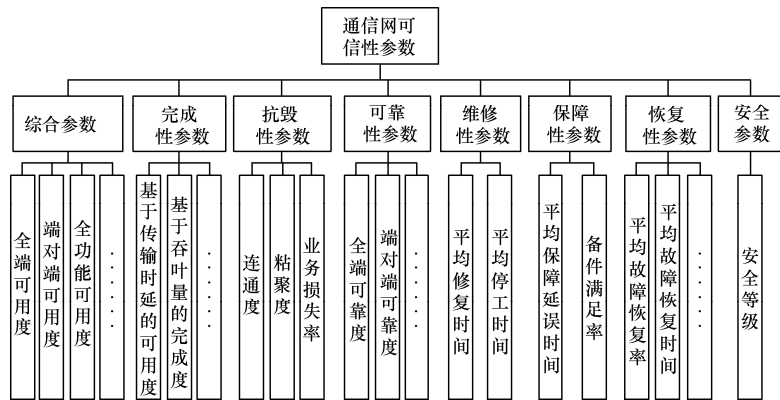


图 10-8 通信网可信性参数体系

1. 综合参数

综合参数整体反映了网络可信性水平，是网络可靠性、维修性和保障性等的综合体现。

(1) 全端可用度 (A_s)

全端可用度是指通信网所有节点对均存在通路，且能够正常通信的平均运行时间与所有节点对存在通路且正常通信的平均运行时间、某一节点对或多个节点对之间不存在通路或不能正常通信的时间的和之比。全端可用度 (A_s) 的计算表达式：

$$A_s = \frac{T_n}{T_n + T_d} \tag{10-6}$$

式中， T_n 表示通信网所有节点对之间均存在通路，且能够正常通信的平均运行时间； T_d 表示通信网某一节点对或多个节点对之间不存在通路或不能够正常通信的时间。

(2) 端对端可用度 (A_p)

端对端可用度是指通信网规定的节点对存在通路，且能够正常通信的平均运行时间与规定节点对存在通路且正常通信的平均运行时间、规定节点对不存在通路或不能正常通信的时间的和之比。端对端可用度 (A_p) 的计算表达式：

$$A_p = \frac{t_n}{t_n + t_d} \tag{10-7}$$

式中， t_n 表示规定的节点对之间存在通路，并且能够正常通信的平均运行时间； t_d 表示规定的节点对之间不存在通路或不能够正常通信的平均运行时间。

(3) 全功能可用度 (A_{fa})

全功能可用度是指通信网规定的功能中，全部功能正常运行的时间与全部功能

正常运行的时间、某一项或多项功能不能正常运行的时间的和之比。全功能可用度 (A_{fa}) 的计算表达式:

$$A_{fa} = \frac{t_{fn}}{t_{fn} + t_{fd}} \quad (10-8)$$

式中, t_{fn} 表示通信网所有功能正常运行的时间; t_{fd} 是指通信网的所有功能中某一项或多项功能不能正常运行的时间。

(4) 主要功能可用度 (A_{fm})

主要功能可用度是指通信网规定的功能中, 主要功能正常运行的时间与主要功能正常运行的时间、主要功能的某一项或多项不能正常运行的时间的和之比。主要功能可用度 (A_{fm}) 的计算表达式:

$$A_{fm} = \frac{t_{fmn}}{t_{fmn} + t_{fmd}} \quad (10-9)$$

式中, t_{fmn} 表示通信网规定的主要功能正常运行的时间; t_{fmd} 表示通信网规定的主要功能中某一项或多项不能正常运行的时间。

(5) 最低功能可用度 (A_{fb})

最低功能可用度是指通信网规定的功能中, 最低功能正常运行的时间与最低功能正常运行的时间、最低功能的一项或多项功能不能正常运行的时间的和之比。最低功能可用度 (A_{fb}) 的计算表达式:

$$A_{fb} = \frac{t_{fbn}}{t_{fbn} + t_{fbd}} \quad (10-10)$$

式中, t_{fbn} 表示通信网规定的最低功能正常运行的时间; t_{fbd} 表示通信网规定的最低功能中某一项或多项不能正常运行的时间。

(6) 一次通信可用度

一次通信可用度是指通信网的节点之间或某两个用户之间, 在一次通信时间内的可用度。其度量方法是: 在特定某一次通信任务时间内, 通信网的特定节点之间或某两个用户之间能够进行通信的时间与能够进行通信时间、不能进行通信时间的和之比。该参数对衡量通信网极其重要的一次通信任务的可用性是有重要意义的。该参数与任务可用度的最大区别在于, 只考虑特定的一次通信任务及对应时间内的系统可用性。

2. 完成性参数

完成性参数是以网络完成业务的质量为依据的参数, 完成性参数称为完成度。

完成度的大小主要由通信网的网元可靠性水平、网络技术、承载的业务及其网络的服务能力、网络流量分布等因素决定。

完成度的表达式:

$$\text{Perf}(B) = \text{Prob}[Y \in B] \quad (10-11)$$

式中, Y 表示业务性能; B 表示业务性能级别。

对于不同类型的通信网, 其完成性度量参数一般不同。比如综合业务数字通信网, 其承载数字、语音、视频等业务, 要求网络的传输时延、吞吐量达到一定的要求, 可选择基于传输时延的完成度 P_S 、基于网络吞吐量的完成度 P_L 等作为其完成性参数。

基于传输时延的完成度 P_S 、基于网络吞吐量的完成度 P_L 的计算方法如下。

(1) 基于传输时延的完成度 (P_S)

假设用户可容忍的网络端到端的最大时延为 T_m , $D_{ij}(S_k, T_m)$ 为网络处于状态 S_k 时, 报文由节点 i 传输到节点 j 而使得时延大于 T_m 的概率。假设时延大于 T_m 的网络状态集合为 Ω , 则网络 i 端到 j 端基于传输时延的完成度 $P_{S,ij}$ 为:

$$P_{S,ij} = \sum_{S_k \in \Omega} [1 - D_{ij}(S_k, T_m)] P(S_k) \quad (10-12)$$

假设 γ_{ij} 为在路径 $i-j$ 上的业务平均到达率, 令在状态 S_k 下传输时延大于 T_m 的全网概率为:

$$D(S_k, T_m) = \frac{\sum_{i,j} \gamma_{ij} D_{ij}(S_k, T_m)}{\sum_{i,j} \gamma_{ij}} \quad (10-13)$$

那么, 基于传输时延的全网完成度为:

$$P_S = \sum_{S_k \in \Omega} [1 - D(S_k, T_m)] P(S_k) \quad (10-14)$$

(2) 基于网络吞吐量的完成度 (P_L)

基于网络吞吐量的完成度 P_L 是指网络的吞吐量超过一个给定阈值 L 的概率。假设一个通信网由 n 个节点和 r 条链路组成, 由于网络部件具有一定的失效概率, 该网络可组合出 $2^{n+r} - 1$ 个失效网络状态和一个所有部件均正常的网络状态。假设所有这些网络状态对应的状态集合为 Ω , S_i 为其中的一个网络状态, 该状态出现的概率为 $P(S_i)$, 那么, 基于网络吞吐量的完成度 P_L 为:

$$P_L = \sum P(S_i) F(S_i) \quad (10-15)$$

式中, $F(S_i)$ 表示网络吞吐量的示意性函数, 其表达式为:



$$F(S_i) = \begin{cases} 1 & \text{如果在状态 } S_i \text{ 下网络的吞吐量} \geq L \\ 0 & \text{否则} \end{cases} \quad (10-16)$$

通信网完成性参数与通信网各网元的状态（故障、降级、正常）、失效模式、性能、承载的业务量等多个因素相关，难以直接采用现场试验进行验证。因此，建议采用仿真试验或者仿真试验与现场试验相结合的方式开展完成性参数验证。

（3）丢包率（ P_D ）

丢包率是指在规定的时间内，丢失的数据包数量与总传输的数据包之比：

$$P_D = \text{丢失的数据包} / \text{发送的数据包} \quad (10-17)$$

（4）接通率（ P_A ）

用户接入网络的接通率是指用户接通网络且认证成功的次数和连接的有效总次数之比，有效总次数应排除用户因素造成的输入错误号码、输入错误账号和密码等的连接次数，接通率 P_A 的计算公式为：

$$P_A = \text{用户接通网络且认证成功的次数} / \text{连接的有效总次数} \quad (10-18)$$

（5）平均误码率

误码率的定义见 GJB 700。平均误码率是指在某一规定的观测时间内（如 168 小时）发生差错的比特数和传输比特总数之比。

（6）呼叫成功率（ P_C ）

呼叫成功率也叫呼叫建立成功率，呼叫成功率 P_C 是在规定的时间内，呼叫建立成功次数（ N_S ）与呼叫请求总次数（ N_R ）之比，其计算公式为：

$$P_C = (N_S / N_R) * 100\% \quad (10-19)$$

3. 抗毁性参数

抗毁性参数包括基于连通性的抗毁性度量参数和基于通信能力的抗毁性度量参数。基于连通性的抗毁性度量参数可采用连通度、粘聚度表示。基于通信能力的抗毁性度量参数，采用业务损失率（ S_a ）表示。

（1）连通度（ CN ）

网络中任意节点对（ i, j ）的连通度 CN_{ij} 为断开（ i, j ）之间所有通路所需去掉的最少节点数，则网络连通度 CN 由下式计算：

$$CN = \min_{i,j} [CN_{ij}] \quad (10-20)$$

（2）粘聚度（ CH ）

网络中任一节点对（ i, j ）的粘聚度 CH_{ij} 为断开（ i, j ）之间所有通路所需去掉的

最少链路数, 则网络粘聚度 CH 由下式计算:

$$CH = \min_{i,j} [CH_{ij}] \quad (10-21)$$

(3) 业务损失率 (S_a)

业务损失率是指通信网在 1 个或多个节点 (或链路) 被毁后, 其剩余业务量的百分数。

$$S_a = \frac{A_{na}}{A_n} \times 100\% \quad (10-22)$$

式中, A_n 表示 n 个节点的通信网的原有业务量; A_{na} 表示 n 个节点的通信网在 1 个或多个节点 (或链路) 被毁后的全网剩余业务量。

4. 可靠性参数

通信网常用的可靠性参数定义及计算方法如下。

(1) 全端可靠度

全端可靠度是指通信网中任意两个节点均能正常通信, 用下式计算网络全端可靠度 $R(G, p_v, p_e)$:

$$R(G, p_v, p_e) = p_v^v \sum_{j=v-1}^e f_j p_e^j (1-p_e)^{e-j} \quad (10-23)$$

式中, G 表示网络; p_v 表示节点的可靠度; p_e 表示链路的可靠度; f_j 表示网络的连通向量; v 表示节点数; e 表示链路数。

(2) 端对端可靠度

端对端可靠度是指从源端 s 通过网络顺利到达终点 t 的概率。如果通信网中一个节点对之间有 m 条最小路径 P_1, P_2, \dots, P_m , 那么网络端到端的可靠度为:

$$R_{st} = P_r \{ \text{从 } s \text{ 到 } t \text{ 至少有一条最小路径} \} = P_r \{ P_1 \cup P_2 \cup \dots \cup P_m \} \quad (10-24)$$

(3) 任务可靠度

任务可靠度是指任务可靠性的概率度量。

(4) 一次通信任务可靠度

一次通信任务可靠度是指通信网的节点之间或某两个用户之间, 在一次通信时间内的可靠度。对所关心的极其重要的一次通信任务, 该项参数及指标是有意义的。

5. 网络可靠性参数的选取依据

参数选取的主要依据包括:



- 网络类型、技术特点、复杂程度、承载的业务类型。
- 考核和验证方法。

参数选取的要求包括：

- 不同类型的网络可信性参数应根据实际情况确定。
- 选择的可靠性、维修性、抗毁性参数应能反映对网络正常运行业务的影响。
- 选择的完成性参数，需要能反映网络主要业务的完成情况，并可通过试验或仿真手段验证。
- 合同中的可用性参数，建议优先选择全功能可用度、主要功能可用度、最低功能可用度要求。

10.6 网络可靠性建模

为了定量分析网络性能，评价网络的可靠性，为改进网络设计提供支持，首先需要建立网络的可靠性模型。

在本书的第 5.3 节，已详细给出了可靠性建模的程序和方法，在此再简略概述一下其要点。

可靠性模型包括可靠性框图和可靠性数学模型两部分内容。可靠性框图应与研究对象的工作原理图及功能框图相协调，原理图则表示对象各单元之间的物理关系，而功能框图表示对象中各单元之间的功能关系。可靠性框图简明扼要、直观地描述了网络对象为完成任务而形成的各种组合（串并联框图）。经典的可靠性框图模型有：串联模型、并联模型、表决模型、非工作储备模型和桥联模型。其中串联模型中组成系统的所有单元中任一单元的故障都会导致整个系统的故障称为串联系统，它是最常用和最简单的模型之一；并联模型中组成系统的所有单元都发生故障时，系统才发生故障称为并联系统，它是最简单的冗余系统；表决模型中组成系统的 n 个单元中，正常单元数不小于 r ($1 \leq r \leq n$)，则系统就不会故障，这样的系统称为 r/n (G) 表决模型，它是工作储备模型的一种形式；非工作储备模型中组成系统的各单元只有一个单元工作，当工作单元故障时，通过转换装置接到另一个单元继续工作，直到所有单元都故障时系统才故障，称为非工作储备系统，又称旁联系统；桥联模型中系统某些功能以冗余形式或替代工作方式实现，是一种既不是串联也不是并联的桥联形式。

为了建立可靠性框图必须全面了解产品完成任务的定义及使用的任务剖面，并给出一般的和专门的假设。

可靠性数学模型是从数学上建立可靠性框图与时间、事件和故障率数据的关系。这种模型的“解”就是所预计的产品可靠性，因此，可靠性数学模型应能根据可靠性

试验和其他有关试验信息、产品配置、任务参数和使用限制等的变化进行及时修改；可靠性数学模型的输入和输出应与产品分析模型的输入和输出关系相一致。

网络可靠性模型较为复杂，与一般系统的可靠性模型相比有很大的不同，本节将详细介绍网络可靠性建模方法。

10.6.1 网络可靠性建模的实施要点

网络不同于普通的研究对象，具有功能众多、结构复杂、故障模式多样等特点，所以对网络进行可靠性建模，需要注意以下要点。

1. 网络可靠性建模依据

可采用 GJB 813 规定的程序和方法建立以产品功能为基础的可靠性模型，可靠性模型应包括可靠性框图和相应的数学模型。可靠性框图应以产品功能框图、原理图、工程图为依据且相互协调。

2. 网络可靠性建模方法的选择

- 如果网络系统各状态之间的转换服从指数分布，并且状态空间不是很复杂（状态数目不多），可采用状态空间法，应用 Markov 模型建立系统可用性模型。
- 如果网络系统各状态之间的转换不服从指数分布，或者系统结构复杂，状态数目很大，可采用随机 Petri 网建立系统可靠性模型。
- 可以建立基于事件驱动的仿真模型，通过仿真方法得到系统的可用度和业务完成度等指标。

应根据需要分别建立产品的基本可靠性模型和任务可靠性模型。

10.6.2 网络可靠性模型分类

根据建模考虑的层次不同，可以将网络可靠性模型分为：基于图论的网络拓扑可靠性模型、基于排队论的可靠性模型、马尔可夫模型、基于 Petri 网的可靠性模型、基于网络性能的网络可靠性模型等。

其中，较早建立的是基于图论的网络拓扑可靠性模型。20 世纪 60 年代，网络可靠性的研究工作主要是以网络的连通性作为网络可靠性标准来研究。

在 20 世纪 80 年代以后，衡量网络可靠性的标准随着实际情况发生了变化。通信网络的广泛应用，使其通信传输量不断增加，网络堵塞和时延增加等性能下降的现象时常发生，这引发了网络性能可靠性的研究。



在网络可靠性研究中,不同领域的网络关注的性能参数有所不同,比如在计算机网络、通信网络中关注更多的是通信时延、丢包数量等性能参数,在交通网络中主要关注的是行程时间、网络容量等性能参数,在电网中考虑的是网络节点发生故障后的抗毁性等,网络性能可靠性研究主要考虑网络性能对网络可靠性和业务可用性方面的影响。

10.6.3 基于排队论的可靠性模型

1. 网络模型的代表

在建立网络模型的任何努力中,其核心议题都是选择适于表示待研系统的抽象机制。网络模型是以图形为基础模型,如限定设备状态和其等价的表示、Petri 网络模型和其他有关方法构成的模型,这种建模形式用于网络协议的确定和检验。所谓检验,即证明协议的正确程度。

网络模型是程序性的模型,即协议被规定为一个用程式的语言写成的交互程序的集合。这种建模方法建立于以下的事实基础,即网络协议具有算法性质,通过设计编程语言能清晰表达所需要的算法。这类模型广泛地用于协议的确定和检验。

网络模型是“加工车间”式的模型。这类模型主要包括排队网络模型和马尔可夫链模型,以及较为复杂的扩展排队网络模型。在这种建模方法中,网络的模型用一组源要素;如通信链路、缓冲器、控制器、集中器和计算机单元(处理器、磁盘和寄存器等)和一组需要使用这些源的加工作业(如数据确认、轮询信息、要执行的规程等)来表示。加工作业在源之间循环,并竞相利用这些源。

这类模型用于分析待建系统的性能,即分析源在系统作业流中被征用所发挥的效能。

2. 基于排队论的网络可靠性模型

排队和排队网络模型属于前面所讲的“加工车间”型模型,而排队网络也正是计算机网络最自然、最直截了当的模型。在这种模型中,网络中的信息流用排队网络的服务来表示。其中,传输设施(链路或集中器)被当成服务中心,缓冲器被当成等待区域,信息为了传输而在等待区域排队。例如图 10-9(a)中 6 节点网络可用如图 10-9(b)所示的排队网络来模拟。

在排队网络模型中,信息到达实际网络的过程(即作业进入网络)特征用到达之间的时间概率分布来表示,不同的传输时间(由于信息长度不同所致)用服务时间分布来表示,作业通过实际网络的路由用被说明的路由链路来模拟。这些路由表明了作业在网络中的每一次排队中,在一级或多级等待区域之间流动的方式。例如图 10-9(a)所示的 2 个信息流 γ_{AF} 和 γ_{DE} (分别在 A、F 节点之间和 D、E 节点之间流动)。相应于这两个信息流的两个路由链,如图 10-9(b)所示,它们表明在节

点 A 进入网络的作业在离开节点 C 之后进到节点 F，而在节点 D 进入网络的信息离开节点 C 之后进到节点 E。

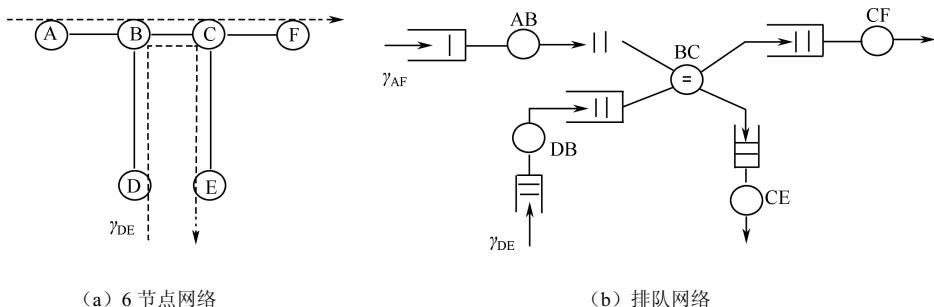


图 10-9 一个计算机网络的排队网络表示

排队网络模型进行数学求解是十分困难的。为此，通常要对它做如下 3 个重要假设：

- 设外部信息到达为泊松过程（用户量越大假设越精确）。
- 假设传输时间依先到先服务的原则（FIFO）呈指数分布。
- 假设排队模型为 Kleinrock 独立假设，该假设为把各种排队的分析隔离开进行的模型引入了足够的独立性，也就是说，一旦知道了每次排队的总信息流速率，如果采用单一的 M/M/1 排队模型，就可求到每段链路的利用率、平均时延、时延分布、平均队长，进而可以求到端到端的平均时延，以及网络中随机信息的平均时延。

事实上，并不是所有的网络和其协议模型都如图 10-9 所示的排队网络模型那样简单。例如，可以从 CF 链的输出端到 AB 链的输入端引一个反馈环路来模拟信息流的控制，或模拟否定确认和信息重发协议。还有，一个排队的调度原则可以不是先来先处理，服务时间可以不是指数分布等。排队论研究的学者已对此类复杂的扩展排队网络模型进行了科学的归纳，提出了一系列数学分析的方法和算法。例如，在计算机网（尤其是广域网）和其协议建模方面非常有用的乘积形式排队网络模型，读者可参考有关专门研究排队网络模型的文献。

10.6.4 马尔可夫链模型

排队网络模型对计算机网和其协议建模十分有用，但对集中器、交换机、随机存储器、环形网络及其协议等并不适用，这时性能模型常常被确定为马尔可夫链模型。

一个马尔可夫链包含若干状态 $i=1, 2, \dots, N$ （代表要模拟的系统状态）和一

个转换矩阵 P , P 要满足从一个状态 i 进入另一个状态 j 的概率 P_{ij} , 而和系统原来的状态无关。

建立马尔可夫链模型的主要目的是为了确定稳态概率矢量 Π , 其分量 Π_i 是系统处于 i 状态的稳态概率, 系统性能度量正是由这些概率值得到。

设有一个随机服务系统 (例如它是一个电话交换系统, 或是一个线束), 以 $\zeta(t)$ 表示系统在时刻 t 的状态, 系统可处于状态 E_1, E_2 等。用 “ $\zeta(t)=i$ ” 表示系统 ζ 时刻 t 以前的情况无关, 即 t 以前的过程只能通过 t 以后的变化体现, 这类数学模型称为马尔可夫过程。

在马尔可夫过程中, 时间和状态两个参数都有可能是离散的或连续的, 因此有 4 种类型的马尔可夫过程, 它们是: 时间和状态都离散的马尔可夫过程; 时间离散、状态连续的马尔可夫过程; 时间连续、状态离散的马尔可夫过程; 时间和状态都连续的马尔可夫过程。

这里, 时间和状态都离散的情况是最简单的一种马尔可夫过程, 称为马尔可夫链。由于通信网交换系统或线束占用状态正是属于时间和状态都离散的情况, 因此可用马尔可夫链的有关方法进行研究。

下面以具有重复呼叫的全利用度系统模型为例, 分析系统的占用状态变化。

设有一容量为 N 的全利用度线束, 进入这个线束的呼叫流有 2 个, 如图 10-10 所示。第 1 个呼叫流是呼叫强度为 λ 的初次呼叫流 (泊松流即为最简单流)。第 2 个呼叫流是重复呼叫流, 假设它来自 k 个有限话源 (重复呼叫用户), 重复呼叫源发出重复呼叫的时间间隔服从强度为 γ 的指数分布, 还假设呼叫平均占用线路时长服从参数为 μ 的指数分布, 平均占用时长 $S=1/\mu$ 。

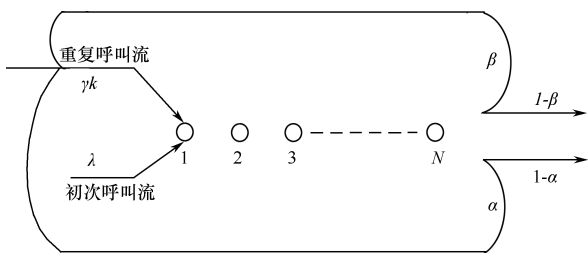


图 10-10 重复呼叫的全利用度系统模型

这样, 系统模型在任何时刻 t 的状态, 要用两个参数来描述: 一个是占用线路数 j ($j=0, 1, 2, \dots, N$), 另一个是重复呼叫话源数量 k ($k=0, 1, 2, \dots$)。下面来讨论系统的状态变化。设系统所处的状态为 (j, k) 。

- 系统有空闲出线 ($j < N$), 在某时刻 t 发生一次初次呼叫, 则系统状态将由 (j, k) 转变为 $(j+1, k)$ 。如果发生的是重复呼叫, 则系统将由 (j, k) 转变为 $(j+1, k-1)$ 。

- 系统无空闲出线($j=N$), 在某时刻 t 发生一次初次呼叫, 则该呼叫用户将以概率 α 成为重复呼叫源, 系统状态将由 (N,k) 转变为 $(N,k+1)$; 或者该呼叫以 $(1-\alpha)$ 的概率消失, 即不再重复呼叫, 系统状态不发生变化, 如果发生的是重复呼叫, 则该呼叫将以概率 β 继续留在重复呼叫话源中, 系统状态不发生变化; 或者该呼叫以 $(1-\beta)$ 的概率离开系统不再返回, 系统状态将由 (N,k) 转变为 $(N,k-1)$ 。
- 呼叫结束其占用时, 系统状态的 j 值减 1。

根据前面所给出的模型, 应用马尔可夫过程的特例——增消随机过程理论, 可以写出重复呼叫的全利用度系统状态概率方程。

根据增消过程理论, 在非常小的时间 τ 内, 给定系统模型状态发生一个初次呼叫的转移概率为

$$\lambda\tau + 0(\tau) \quad (10-25)$$

发生一个重复呼叫的转移概率为

$$k\lambda\tau + 0(\tau)$$

有一个设备被释放的转移概率为

$$j\mu\tau + 0(\tau)$$

在 τ 时间内, 没有发生初次呼叫, 没有发生重复呼叫, 也没有呼叫释放设备的转移概率为

$$1 - (\lambda + k\gamma + j\mu)\tau + 0(\tau)$$

在设备全忙的条件下, 即 $j=N$, 如果在 τ 时间内发生一个重复呼叫, 那么它将以概率 $(1-\beta)$ 离开系统, 从而使重复呼叫源数减 1。发生这种状态变化的转移概率为

$$(1-\beta)\gamma k\tau + 0(\tau)$$

如果发生的是初次呼叫, 则它以概率 α 留在系统内, 成为重复呼叫源, 发生这种状态变化的转移概率为

$$\alpha\lambda\tau + 0(\tau)$$

在 τ 时间内状态 (N,k) 不发生变化的概率为

$$1 - (\alpha\lambda + \gamma k(1-\beta) + \mu N)\tau + 0(\tau)$$

显然, 系统经时间 $(t, t+\tau)$ 由相邻状态进入状态 (j,k) , 在 t 时刻的状态必定是 4 个状态中的一个, 图 10-11 (a) 表示了这 4 个状态之间的转移关系和相应的条件转移概率。图中删去了转移概率中的高阶无穷小 $0(\tau)$ 。若将 t 时刻系统处于状态 (j,k) 的概率用 $p(j,k,t)$ 表示, 则发生这 4 个状态的概率可分别写为 (结合图来看)

$$p_1(j,k,t+\tau) = \lambda\tau p(j-1,k,t) + 0(\tau)$$

$$p_2(j,k,t+\tau) = \gamma(k+1)\tau p(j-1,k+1) + 0(\tau)$$



$$p_3(j, k, t + \tau) = \mu(j+1)\tau p(j+1, k, t) + 0(\tau)$$

$$p_4(j, k, t + \tau) = [1 - (\lambda + k\gamma + \mu j)\tau]p(j, k, t) + 0(\tau)$$

由于发生状态 (j, k) 的这4个事件是互不相容的, 因此有:

$$p(j, k, t + \tau) = \sum_{i=1}^4 p_i(j, k, t + \tau) \quad (10-26)$$

式(10-26)中不包括 $j=N$ 的情况, 也就是 N 条线全忙的情况。经过 τ 时间使系统在时刻 $(t+\tau)$ 处于状态 (N, k) 的所有可能事件有5个, 图10-11(b)表示了这些状态的转移关系, 相应的条件转移概率可分别为:

$$p_5(N, k, t + \tau) = \alpha\lambda\tau p(N, k-1, t) + 0(\tau)$$

$$p_6(N, k, t + \tau) = (1 - \beta)\gamma(k+1)\tau p(N, k+1, t) + 0(\tau)$$

$$p_7(N, k, t + \tau) = \gamma(k+1)\tau p(N-1, k, t) + 0(\tau)$$

$$p_8(N, k, t + \tau) = \lambda\tau p(N-1, k, t) + 0(\tau)$$

$$p_9(N, k, t + \tau) = [1 - (\alpha\lambda + Nk(1 - \beta) + \mu N)\tau]p(N, k, t) + 0(\tau)$$

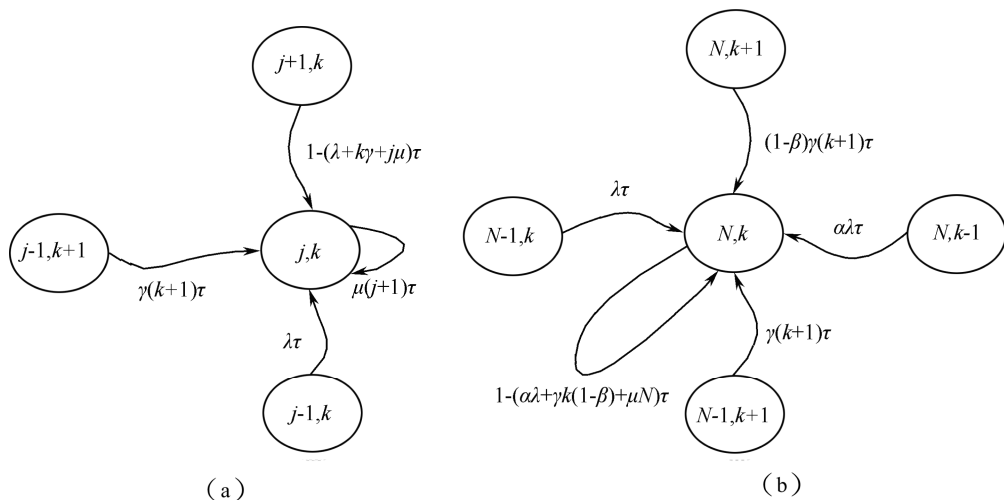


图 10-11 状态转换关系图

上述5个事件的概率即为系统在时刻 $(t+\tau)$ 处于状态 (N, k) 的概率:

$$P(N, k, t + \tau) = \sum_{i=5}^9 p_i(N, k, t + \tau) \quad (10-27)$$

式(10-26)和式(10-27)构成了描述系统状态的方程组, 该方程组经变换可得到如下描述。

重复呼叫系统在统计平衡条件下状态的代数方程组为:

$$\begin{cases} [\lambda + \mu j + Nk] p(j, k) = N(k+1) p(j-1, k+1) + \lambda p(j-1, k) + (j+1) \mu p(j+1, k) \\ j = 0, 1, 2, \dots, N-1; k = 0, 1, 2, \dots \\ [\alpha \lambda + Nk(1-\beta) + \mu N] p(N, k) = \alpha \lambda p(N, k-1) + (1-\beta) N(k+1) p(N, k+1) + \\ \gamma(k+1) p(N-1, k+1) + \lambda p(N-1, k) \sum_{k=0}^{\infty} \sum_{j=0}^{\infty} p(j, k) = 1 \end{cases} \quad (10-28)$$

线性方程组式(10-28)完全描述了所研究的重复呼叫系统。

在一般情况下状态方程组没有简单的解析解,但有一些近似的数值方法,如可以通过查数值的方法(借助计算机)做出表格。通过建立系统状态联立方程组并求解即可求到稳态概率矢量 Π 。

10.6.5 考虑加权因子的可靠性模型

1. 考虑加权因子的全网可靠性模型

系统的主要功能是确保在一次战役任务时间内各节点(用户)的通信业务畅通,因此,我们可以将系统可靠性测度指标定义为任意两个节点(或用户)之间的可靠性指标集合,即以综合的端-端可靠性来反映系统整体可靠性水平。要求同系统指标联系起来,就是用户端-端可用性指标。因为用户具有不同的等级,他们对系统可靠性要求也就不同,为更客观地评价系统的可靠性,给出如下一个加权的通信网总体可靠性模型为:

$$R_s = \sum_{ij} (W_{ij} R_{ij}) / W \quad (10-29)$$

其中, $W = \sum_{ij} W_{ij}$, R_s 为系统可靠性, W_{ij} 为节点 i 与节点 j 之间的可靠性加权因子; R_{ij} 为节点 i, j 之间的通信可靠性,或者说(在不致引起混淆的情况下)是用户 i, j 之间的通信可靠性。

式(10-29)中的 W_{ij} 取值取决于节点 i 与节点 j 之间的信息流量,以及它们之间的通信中断(故障)对通信网完成任务的影响程度,这是一个军事或工程判断问题。一般来说,重要的节点或用户业务量大,因此 W_{ij} 的取值可以按如下公式求得:

$$W_{ij} = E_{ij} + E_{ji} \quad (10-30)$$

其中, E_{ij} 和 E_{ji} 分别为 i 到 j 和 j 到 i 的业务流量。

本模型的实质是将系统主要功能表示为所有用户通信的集合,将通信网可靠性

指标 R 定义为:

$$R = \begin{bmatrix} R_{11} & R_{12} & \cdots & R_{1n} \\ R_{21} & R_{22} & \cdots & R_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ R_{n1} & R_{n2} & \cdots & R_{nn} \end{bmatrix} \quad (10-31)$$

即节点(用户)间通信的可靠性矩阵。它表达了所有节点(用户)间通信的可靠性指标集合。

可靠性模型采用节点间可靠性指标的加权均值而不是简单的算术平均值,是因为各节点之间通信的中断对系统完成任务所造成的影响是不一样的。

在给出的通信网可靠性数学模型中,对于所有的 $i, j (i < j = 1, 2, \cdots, n)$, R_{ij} 对应的结构模型一般都包含了通信网模型,从宏观角度来分析,通信网的失效(或毁坏)将影响所有用户的通信,所以通信网起着非常重要的作用,提高通信网的可靠性可以提高所有用户间的通信可靠性,但对任意一对用户来说提高幅度可能并不大。如果要求大幅度提高某些特别重要用户之间的可靠性,则需要采取其他措施,因此该模型对进行系统可靠性设计和优化设计是很有用的。

2. 一种基于最小路集的高效工程算法

针对现有可靠性评价方法存在过多冗余运算、花费大量的存储空间等问题,项目组提出了一种高效的通信网可靠性算法用于通信网的可靠性评价。

该算法的思路是基于最小路集,根据因式分解法原理,将利用分割路集的操作代替了对分图的操作,但是并不需要对所有分割路集进行记录,而是依据自然过程对路径标号进行操作,其基本原理是:

$$\{S\} = p_x \{S_p\} + q_x \{S_q\} \quad (10-32)$$

其中, S 是系统所有最小路径的集合; x 为系统任意部件; p_x 是 x 成功的概率,算法中由它引出的点称为 p 节点; q_x 是 x 失效的概率,算法中由它引出的点称为 q 节点; S_p 和 S_q 分别表示相应 p 节点或 q 节点导出的系统所有最小路径的集合,它对应着相应节点的状态; $\{S_p\}$ 和 $\{S_q\}$ 表示从相应 p 节点或 q 节点出发导致系统成功的不交事件概率之和,或者在不引起误解的情况下系统成功的路径集合。

算法处理过程本身类似于对具有 p 节点和 q 节点的二叉树的操作,但这样的一棵树,程序并不需要产生,只要想象其结构即可,因为所有的 p 节点状态或 q 节点状态都可以通过最近的第一个前驱 p 节点状态得到。

10.6.6 基于 Petri 网的可靠性模型

Petri 网最早由 C.A.Petri 于 1962 年在其博士论文中提出,它是一种系统描述和分析的工具。Petri 网在模型描述时具有以下特点:

- Petri 网是一个网状结构信息流模型,可以对系统进行数学和图形的描述、分析,作为一种数学工具,它可以建立系统状态方程、代数方程以及系统行为的模型,可以对其进行量化计算和验算。作为一种图形处理工具,在建立模型过程中既直观又形象,便于表达和建模。
- 对具有并发、异步、分布及并行特征的系统有很好的适用性。
- 可以较好描述系统的时间特性、不确定性(指人为因素等)和系统的随机特性。
- 可以使用标记来模拟和仿真系统的动态行为。

对于一个系统,如果能够构造出它的 Petri 网模型,并对其进行彻底分析,就能揭示出被模拟系统在结构和动态行为方面的许多重要信息。抽象地说, Petri 网是由系统状态节点、事件迁移节点和迁移方向连接成的二元有向图。如果将系统输入位置节点和输出位置节点所形成的集合设为 P ,转移节点集合为 T ,所有转移方向有向弧集合为 F ,则 Petri 网络模型可采用三元素组 (P,T,F) 表示。如果对 Petri 网的定义加以扩展,就可以用来描述通信网内各实体和动态过程。目前 Petri 网已用于设计和开发通用的通信网络模拟系统。

10.6.7 基于信息动力学的网络性能可靠性模型

网络性能可靠性的测度主要包括有效性、完成性、可行性等,它们都是在网络部件失效的条件下,利用网络在性能约束下完成业务的概率来度量其性能可靠性。实际上,通信网络的性能下降往往是由信息流变化引起的。

该模型首先基于信息流动力学建立通信网络的流量模型,在此基础上定义信息流传输时延和分组丢失率表征网络性能可靠性的指标,建立对应的可靠性模型。

1. 建立网络信息流模型

在计算机网络的背景下,做如下几点假设:计算机网络大多采用光纤作为传输媒介,制约信息流传输的瓶颈是节点,因此不考虑边对信息流传输的影响;网络节点分为收发节点和转发节点,收发节点仅负责数据分组的发送和接收,转发节点仅负责数据分组的转发;不考虑信息流传输的方向性;网络采用单约束单路由方式;

不考虑网络硬件和软件的不可靠性。

在上述假设的基础上，建立一个计算机网络的信息流模型，详细描述如下：在 t 时刻，任意 2 个收发节点 v_i 、 v_j 节点， v_i （或 v_j ）将 $S_{ij}(t)$ 个数据分组向节点 v_j （或 v_i ）发送，这些数据分组按照一定的路径 $P_{ij}(t)$ 在网络中传输， $P_{ij}(t)$ 是根据网络在 $t-1$ 时刻的负载情况以及在 $[t-1, t]$ 单位时间内加载的信息流情况而选择的性能最优路径，记为信息流 $flow_{ij}(t) = (S_{ij}(t), P_{ij}(t))$ ；假定每个转发节点的数据分组转发能力是有限的，即在 t 时刻，任意转发节点 v_k 只能将 $C_k(t)$ 个数据分组传到下一个节点；如果一个数据分组到达转发节点时，已经有数据分组在等待转发，那么新到达的数据分组将排在队列的末尾，转发节点 v_k 的负载变化如下：

$$\begin{cases} W_k(t) = N_k(t) + Q_k(t-1) \\ Q_k(t-1) = \begin{cases} 0 & W_k(t-1) \leq C_k(t-1) \\ W_k(t-1) - C_k(t-1), & \text{否则} \end{cases} \\ N_k(t) = \sum_{v_i \neq v_j \in V_{\text{send-receive}}} (S_{ij}(t) \times \sigma_{ij}(k, t)) \end{cases} \quad (10-33)$$

其中， $\sigma_{ij}(k, t)$ 是指 t 时刻，信息流 $flow_{ij}(t)$ 的传输路径 $P_{ij}(t)$ 是否经过节点 v_k 。当 $P_{ij}(t)$ 不经过节点 v_k ，则 $\sigma_{ij}(k, t) = 0$ ；当 $P_{ij}(t)$ 经过节点 v_k ，则 $\sigma_{ij}(k, t) = 1$ 。 $N_k(t)$ 是指 t 时刻，新到达节点 v_k 的数据分组数量。 $W_k(t)$ 是指 t 时刻，需要节点 v_k 转发的数据分组数量。 $C_k(t-1)$ 是指 $t-1$ 时刻，节点 v_k 能够转发的数据分组数目。 $Q_k(t-1)$ 是指 $t-1$ 时刻，节点 v_k 未能转发的数据分组数量。

2. 建立网络可靠性模型

网络性能是通过网络传输信息流的性能来体现的，信息流的性能是由信息流传输过程中经过的每个转发节点的工作状态（自由态，拥塞态）决定。随着信息流路由 $P_{ij}(t)$ 或发包率 $S_{ij}(t)$ 的变化，在转发节点 v_k 等待转发的数据分组数量 $W_k(t)$ 就会不断变化，使得转发节点不断在自由态和拥塞态之间发生相变。当 $W_k(t) \leq C_k(t)$ ，数据分组不需要排队等待，则节点 v_k 能快速转发数据分组；当 $W_k(t) > C_k(t)$ ，由于节点 v_k 的数据分组转发能力是有限的，则数据分组需要排队等待，这将增加数据分组的时延、分组丢失率等，进而降低信息流的性能，影响整个网络的性能可靠性。

在 t 时刻，节点 v_k 转发数据分组的时延 $D_k(t)$ 、分组丢失率 $L_k(t)$ 与 $W_k(t)$ 的关系如下：

$$D_k(t) = \begin{cases} d_k(t) & W_k(t) \leq C_k(t) \\ d_k(t) \times \left(\frac{W_k(t)}{C_k(t)} \right)^\alpha & W_k(t) > C_k(t) \end{cases} \quad (10-34)$$

$$L_k(t) = \begin{cases} I_k(t) & W_k(t) \leq C_k(t) \\ I_k(t) \times \left(\frac{W_k(t)}{C_k(t)} \right)^\beta & W_k(t) > C_k(t) \end{cases} \quad (10-35)$$

其中, $d_k(t)$ 、 $I_k(t)$ 是节点 v_k 在 $W_k(t) \leq C_k(t)$ 时, 转发数据分组的时延和分组丢失率, 由硬件性能决定。 α 、 $\beta > 0$, 是队列长度对数据分组性能的影响因子。任意 2 个收发节点 v_i 、 v_j , 它们之间信息流 $flow_{ij}(t)$ 的时延、分组丢失率等 QoS 要求记为 $D_{ij}(t)$ 、 $L_{ij}(t)$, 其中 $P_{ij}(t) = \{v_i, v_1, \dots, v_k, \dots, v_l, v_j\}$ 可通过路由策略确定, 因此从 v_i 传输到 v_j 的信息流的性能可靠性就可确定。

在 t 时刻, 信息流 $flow_{ij}(t)$ 的性能可靠性如下:

$$\begin{cases} Delay_R_{ij}(t) = \prod_{k=1, v_k \in P_{ij}(t)}^l e^{-\gamma \times f_k(t)} \\ Loss_R_{ij}(t) = \prod_{k=1, v_k \in P_{ij}(t)}^l e^{-\gamma \times g_k(t)} \end{cases} \quad (10-36)$$

其中, $\gamma > 0$, $f_k(t)$ 、 $g_k(t)$ 分别为

$$\begin{cases} f_k(t) = \sum_{s=1, v_s \in P_{ij}(t)}^k D_s(t) / D_{ij}(t) \\ g_k(t) = \prod_{s=1, v_s \in P_{ij}(t)}^k L_s(t) / L_{ij}(t) \end{cases} \quad (10-37)$$

γ 是关联参数, 反映节点与路径上游各节点的关联性。 $f_k(t)$ 、 $g_k(t)$ 反映了网络在路径 $P_{ij}(t)$ 上传输信息流的性能(时延, 分组丢失率)与用户要求的性能(时延、分组丢失率)的差异程度, 即网络传输信息流的质量水平。

在 t 时刻, 网络 G 的性能可靠性为

$$\begin{cases} Delay_R_G(t) = \frac{\sum_{v_i \neq v_j \in V_{send-receive}} Delay_R_{ij}(t)}{Num_flow(t)} \\ Loss_R_G(t) = \frac{\sum_{v_i \neq v_j \in V_{send-receive}} Loss_R_{ij}(t)}{Num_flow(t)} \end{cases} \quad (10-38)$$

其中:

$$Num_flow(t) = \sum_{v_i \neq v_j \in V_{send-receive}} \|flow_{ij}(t)\| \quad (10-39)$$

这是网络 t 时刻产生信息流的数目, 且

$$\|flow_{ij}(t)\| = \begin{cases} 1 & S_{ij}(t) > 0 \\ 0 & S_{ij}(t) = 0 \end{cases} \quad (10-40)$$

在一个流量变化周期内，网络性能可靠性为

$$\begin{cases} Delay_R(G) = \frac{\sum_{t \in [0, T]} Delay_R_G(t)}{T} \\ Loss_R(G) = \frac{\sum_{t \in [0, T]} Loss_R_G(t)}{T} \end{cases} \quad (10-41)$$

10.6.8 交通网行程时间可靠性模型

行程时间可靠度是用来反映出行时间的变异性，是一个非常重要的衡量路网可靠性的指标。它指的是在具体的服务水平下和给定的时间内，从起点到终点出行成功的概率。这一定义可以很好地用来估计日常流量变动下的网络可靠度。

路径的出行时间由各路段的出行时间决定，其期望值和方差等于各路段出行时间的期望值和方差之和，如式（10-42）所示：

$$T = N \left(\sum_{a \in p} u_a, \sum_{a \in p} \sigma_a^2 \right) \quad (10-42)$$

式中， T 为路径的出行时间； u_a 为路段 a 的出行时间的期望值； σ_a^2 为路段 a 的出行时间的方差。

由式（10-42）给出的行程时间定义，可得到行程时间可靠度（行程时间小于某一给定阈值的概率）模型：

$$P(T \leq t) = \Phi \left(\frac{t - \sum_{a \in p} u_a}{\sqrt{\sum_{a \in p} \sigma_a^2}} \right) \quad (10-43)$$

式中， u_a 表示路段 a 的平均行驶时间（h）； t 表示路径行驶时间（h）； σ_a 表示路段 a 行驶时间的标准差； r 表示出行所经过路段组成的集合。

10.6.9 相继故障传播模型

考虑到实际网络中节点的处理能力有限，网络中一旦少数节点或链路故障，可能会通过节点之间的耦合关系引起其他节点发生故障，形成“连锁反应”，即“相继故障”，有时也称为“雪崩”，因此前人也对故障传播规律建立了很多模型进行描述，如

负荷-容量模型、二值影响模型、沙堆模型、OPA 模型、CASCADE 模型等。

- 负荷-容量模型通过考虑网络中节点和链路的容量、负荷之间的关系判定故障，一旦节点或链路故障，便将其负荷按一定策略分配到其他节点或链路，如负荷超过容量则发生相继故障，这实际也是系统中“应力-强度干涉模型”的一个实例。
- 二值影响模型假设网络中的节点具有二态性（故障/正常），假定一个节点的相邻节点中故障节点的数量超过某一阈值，则认定该节点也故障，由此模拟网络中的相继故障现象。
- 沙堆模型对每个节点赋予一个“高度”（类似于负荷）的概念，当节点高度大于其给定阈值时（将这一状态比喻成沙崩的临界状态，称为自组织临界），则将其高度“倾倒”给其部分相邻节点，由此模拟相继故障。
- OPA（最优潮流方法）模型是对电网相继故障的模拟，通过模拟电网节点或链路故障后的功率分配，再判断其他节点或链路是否发生相继故障。
- CASCADE 模型是假设网络初始处于正常状态，由于受到扰动后有的节点发生故障，并将固定大小的负荷传递给其他节点，由此模拟相继故障。

Lubos Buzna 和翁文国等人先后提出了网络系统中的灾害传播模型，对网络中的动力学规律进行研究，并探究了不同节点修复能力下灾害传播的临界特性。大连理工大学的郭天柱和中国矿业大学的李泽荃等人在此基础上分别研究了网络中心性对灾害传播的影响，这些研究结果对于灾害预防和灾害应急管理具有重要意义，但是该模型中假设节点只有两种状态：正常和故障，而且没有考虑节点自身的动力学特性。

在社会和计算机网络方面，继 Ross 于 1915 年提出确定型的 SIS 模型之后，SIR 疾病传播模型、SEIR 疾病传播模型，以及 SIRS、SEIS-V、SIRaRu 模型和相应的改进模型陆续提出，对网络中的故障传播规律，网络稳定性等问题进行了相应的研究。

此外，还有部分研究学者利用元胞自动机这种在时间维、空间维和状态维都是离散的方法对网络中的故障传播过程进行建模，通过数值仿真对网络中故障传播的离散时间过程进行了相应的探索。

10.7

网络可靠性计算

网络可靠性计算方法可以分为解析算法和仿真算法两类。

10.7.1 解析算法

解析算法是通过给定网络中各个节点和链路的可靠度/故障率，采用状态枚举法、容斥原理法、不交积和法、因子分解法、图变换法、定界法等，计算网络连通可靠度。基本思想如表 10-1 所示。

表 10-1 网络可靠性计算的经典解析算法

算法名称	基本思想	说明
状态枚举法	假设网络元件存在正常与故障两种状态，通过枚举出网络正常的所有元件状态而计算相应的可靠度	该方法最早于 1956 年由 Moore 和 Shannon 提出
容斥原理法	将网络可靠度表述为全部最小路集的并（或将网络不可靠度表示为全部最小割集的并），然后采用容斥原理去掉相容事件相交的部分，从而计算相应的可靠度	最早于 1978 年由 Satyanarayana 和 Prabhakar 提出
不交积和法	将网络可靠度表述为全部最小路集的并（或将不可靠度表示为全部最小割集的并），再求解这个并的不交和，从而计算相应的可靠度	最早于 1979 年由 Abraham 提出
因子分解法	选择网络中的一个元件，按照其可靠与不可靠逐步进行分解，从而迭代获得网络可靠度	最早于 1958 年由 Moskowitz 提出
图变换法	按照某种规则简化网络，使原问题的可靠性变大或变小而得到可靠性指标的上界或下界，是一种通过牺牲精度而降低计算难度的算法	典型的图变换法有△-Y 型简化法、串并联简化法、多边形→链简化法、三角形简化法等
定界法	通过分析网络的组合结构，利用数学方法给出可靠性指标的绝对上界或下界	最著名的要数 Esary 和 Proschan 于 1963 年提出的 Esary-Proschan 界

由于网络的复杂性和随机性，一般很难给出网络流通可靠性参数的解析计算模型，该方法仅适用于连通可靠性参数的计算。随着计算机技术的发展，研究人员逐渐开始关注以计算机和应用软件为工具的可靠性仿真算法。

10.7.2 仿真算法

由于网络使用会受到元件故障、网络流变化、路由策略等因素的影响，网络的复杂性和随机性给反映网络使用的可靠性分析带来了很大的困难，难以建立流通可靠性的理论模型，现有的研究成果都是基于模拟或统计数据的分析。

仿真方法是当前乃至未来网络系统可靠性评估的主要途径，通过构建网络系统可靠性模型，构建业务、故障、维修以及其他随机性参数模型，真实模拟网络中的各种动力学行为，统计分析相应的可靠性参数。当前关于通信网系统可靠性仿真方

法按照网络建模方式大致分为蒙特卡洛仿真和状态机仿真两大类。

- 蒙特卡洛仿真方法的主要思想是通过对实际问题的分析构造随机事件，使得它的某种概率统计量就是问题的解，对该随机事件进行抽样并计算出问题的结果，这是一种应用随机抽样获得数学或物理问题解的概率统计方法。蒙特卡洛仿真主要利用当前通用的通信网性能仿真平台和工具，如 OPNET、NS2、OMNEST 等，依据实际网络拓扑结构、通信协议以及业务流程等，模拟构造通信系统的可靠性评估网络模型，通过输入网络流量、故障分布以及维修等随机参数，通过蒙特卡洛仿真统计得到相关可靠性参数。
- 状态机仿真针对通信网中的复杂离散事件，将网络的动态行为通过状态机进行描述，通过统计相关状态参数分析系统可靠性水平，常见的是基于 Petri 网的网络可靠性建模仿真方法。Petri 网是进行离散事件动态系统建模与仿真的有力工具，它可以清晰自然地描述系统中的各种逻辑关系，以及常见的同步、资源共享、竞争、冲突等现象。但通常的 Petri 网的描述能力仍然有限，对多节点链路构成的复杂网络系统建模时，容易造成状态组合爆炸现象，因此，有关学者又提出了有色 Petri 网（CPN）、随机 Petri 网（SPN）、面向对象的 Petri 网（OOPN）等高级 Petri 网模型，有的模型已用于进行网络系统可靠性问题的建模与分析，表现出了一定的优越性。

10.7.3 网络可靠性计算方法比较

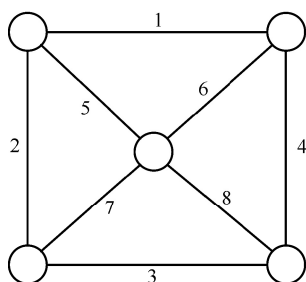
和普通系统一样，在计算网络可靠性的方法上，也分为三大类：数学解析方法、仿真方法和试验方法，三种方法在实现难易程度、精确度、成本和适用网络方面各有优缺点，所以，在对一个网络的可靠性进行分析评价时，应该根据网络的规模，综合考虑成本限制、精确度要求，选择合适的方法，如表 10-2 所示。

表 10-2 网络可靠性计算方法比较

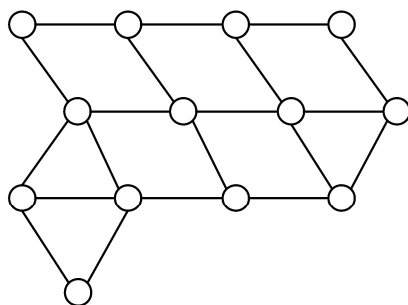
方法	实现难易程度	精确度	成本	适用网络
数学解析方法	最难	较准确	一般	小规模网络
仿真方法	简单	误差大	成本最低	不限制
试验方法	较难	最准确	成本最高	小规模网络

【例 10-1】网络可靠性仿真的案例分析

如图 10-12（a）所示是 5 个节点、8 条链路的简单网络，图中数字是链路的编号。如图 10-12（b）所示是 13 个节点、20 条链路的较为复杂的网络。



(a) 简单网络



(b) 较复杂的网络

图 10-12 网络图

我们先对简单网络进行说明。这一网络生成 45 棵树，每棵树由 4 条链路构成。整个树集如表 10-3 所示。

表 10-3 网络树集表

1235	1236	1237	1238	1245	1246	1247	1248
1357	1358	1367	1368	1457	1467	1478	1578
2368	2456	2458	2457	2478	2568	2678	3456
1258	1268	1278	1345	1346	1347	1348	
1678	2345	2346	2347	2348	2356	2367	
3457	3458	3567	3568	4567	4578	5678	

设第 1、2、3、4 号链路的失效率均等于 0.016 25/h，第 5、6、7、8 号链路的失效率均等于 0.028 76/h，设网络的任务持续时间为 10h。

当用解析方法求解网络在 10h 内的可靠度时，需要按照下列表达式进行计算：

$$\begin{aligned}
 R_s = (t=10) = & \sum_{i=1}^{45} P(T_i) - \sum_{i_1 \neq i_2} \binom{45}{2} P(T_{i_1} T_{i_2}) + \sum_{i_1 \neq i_2 \neq i_3} \binom{45}{3} P(T_{i_1} T_{i_2} T_{i_3}) \\
 & \dots (-1)^{j+1} \sum_{i_1 \neq i_2 \dots \neq i_j} \binom{45}{j} P(T_{i_1} \dots T_{i_j}) + \dots (-1)^{45+1} \sum_{i=1}^{45} P(T_i)
 \end{aligned}$$

式中： T_i ——第 i 棵树；

$P(T_i)$ ——第 i 棵树正常工作的概率；

$\sum_{i=1}^{45}$ ——表示和式的项数等于 $\frac{45!}{i!(45-i)!}$ 项。

计算的结果为网络在 10h 工作中的可靠度等于 0.969 813。

当用可靠性仿真时，根据 8 条链路的失效率及其分布，由计算机产生的某一次

8 条链路正常工作的随机小时数依次为 126.24、3.56、183.8、164.22、25.87、50.66、1.91、31.21。这就是说,第 1、3、4、5、6、8 条链路在 (10h) 任务持续时间内工作是可靠的,而第 2、7 两条链路在任务持续时间内发生了失效,从树集判断,实际上只要第 1、3、4、5 链路正常工作就能保障网络连通了,因此,这一次仿真试验是成功的。如果在另一次仿真试验中得到的 8 条链路工作的随机数是 6.92、450.04、60.38、0.97、29.76、3.56、4.67、55.76,这说明第 2、3、5、8 链路在 10h 内工作可靠;而第 1、4、6、7 链路发生了失效;2358 在树集中是不存在的,因此网络发生了失效,在此情况下,有一个节点已经脱网。当仿真进行了 5 万次,其中有 48 369 次成功,因此仿真得出的结果是网络可靠度为 0.967 38,与解析的精确解比较,失效概率的误差在 8% 左右。

由此可见,可靠性仿真比之解析方法的计算过程的耗时大幅度下降,对于简化复杂网络分析则更加显著。

如图 10-12 (b) 所示为 13 个节点、20 条链路的网络,当每条链路的可靠度均为 0.90,网络的可靠度用解析法得到的精确解等于 0.956 550 587 8,用仿真得到的网络可靠度等于 0.954 37,误差在 5% 范围内。

10.8 网络可靠性评估

10.8.1 可靠性评估方法概述

从工程实现方式上,网络可靠性评估方法主要分为如下几种。

1. 基于图论、概率论等理论的数学解析方法

数学解析方法主要解决了基于网络拓扑和网络部件故障下的网络连通性问题,包括精确计算和近似计算两种算法。

2. 基于随机事件的计算机仿真计算方法

仿真方法通过构建网络模型、业务模型、故障及维修事件模型,可对网络连通可靠性和网络性能可靠性进行仿真,主要采用蒙特卡洛仿真方法,部分研究也将 Petri 网理论引入网络可靠性仿真研究中。

3. 基于真实试验网络的现场可靠性统计试验验证方法

试验验证方法构建真实试验网络,施加任务剖面,基于传输需求评估网络性能可靠性。



上述三种方法各有优劣，一般工程实践中采用多种方法相结合的形式。

综合评价方法研究主要是解决单一参数无法综合衡量网络可靠性，单一评估方法的结论可信度差的问题。当前部分研究学者也试图采用层析分析法、模糊综合评价法、人工神经网络法等得到网络可靠性的综合评估结论。

任务剖面技术是网络系统可靠性评估的关键技术之一。由于网络系统的网络规模、拓扑结构、用户规模、通信需求、管理方式、使用地域等多种因素导致任务剖面复杂多变。任务剖面技术研究就是要建立一套从实际环境下提取典型任务剖面的方法，确立网络任务剖面架构，并研究相对应的任务剖面加载技术，其核心是确定网络系统的业务剖面，包括业务种类、频度、分布、流向、流量等研究内容。

根据评估时关注的网络层次不同，可以将网络可靠性评估分为：

- 网络连通可靠性评估，指的是仅考虑网络拓扑结构，将“网络实现连通功能的概率”作为可靠性度量。
- 网络容量可靠性评估，它在考虑网络是否连通的基础上，还考虑了网络中链路和节点的容量，将“存在满足一定流量需求的连通路路径的概率”作为可靠性度量。
- 网络性能可靠性评估，关注的是网络性能的动态变化对可靠性的影响，多以“某些性能参数不超过其规定阈值的概率”作为可靠性的度量。
- 以业务为中心的网络可靠性综合评估，综合考虑了网络的连通可靠性、容量可靠性和性能可靠性，将“网络对某业务的支持能力”作为业务可靠性的度量。

10.8.2 连通可靠性评估

网络可以抽象为由一组节点集与一组链路集构成的图。1955 年，Lee 在“Analysis of Switching Networks”（交换网络分析）一文中，定义了以“能实现连通功能的概率”为度量的端可靠度，首次使用了以连通为规定功能的可靠性指标。连通可靠性也是最早提出的网络可靠性指标，根据网络有无指定的源点可以分为有源网络与无源网络。

有源网络可靠性指标分为 3 类：

- ST 可靠度（源点 S 与终点 T 保持连通的概率）。
- SK 可靠度（源点 S 与特定的端点集 K 保持连通的概率）。
- SAT 可靠度（源点 S 与网络中所有其他端点保持连通的概率）。

无源网络可靠性指标也分为 3 类：

- 两端可靠度（网络中两个端点间保持连通的概率）。
- 端可靠度（网络中 k 个端点间保持连通的概率）。
- 全端可靠度（网络中所有端点保持连通的概率）。

计算网络连通可靠性的经典解析算法往往做如下假设：

- 链路只有故障、正常两种状态。
- 网络中链路故障的概率是统计独立的。

经典评估算法有 5 种，如表 10-4 所示。它们往往面临计算复杂度随网络节点数增加而指数增长的“组合爆炸”问题，因此只适用于节点数较少或者网络拓扑结构特殊的情况。

表 10-4 连通可靠性评估经典算法

算法名称	算法实现原理
状态枚举法	通过枚举出网络正常的所有元件状态而计算相应的可靠度
容斥原理法	将网络可靠度表述为全部最小路集的并（或将网络不可靠度表示为全部最小割集的并），然后采用容斥原理去掉相容事件相交的部分，计算相应的可靠度
不交积和法	将网络可靠度表述为全部最小路集的并（或将网络不可靠度表示为全部最小割集的并），再求解这个并的不交和，计算相应的可靠度
因子分解法	选择网络中的一个元件，按照其可靠与不可靠逐步进行分解，从而迭代获得网络可靠度
图形拓扑方法	主要指简化图形的精确算法。最早针对串并联网络，以“将串联链路的可靠度相乘、并联链路的可靠度相加”为原则简化图形

为了解决以上组合爆炸问题，之后的可靠性工作者们又提出了一些近似算法，如图变换法（简化网络得到可靠性指标的上 / 下界）、定界法、蒙特卡洛法等。

定界法的原理是先扫描所有的最小割集，通过比较割集的失效概率找出薄弱割集（Weak Cutset），再通过连续截断来近似估算一个预先给定绝对误差大于 0 的网络的全终端可靠性（给出可靠度上界及下界）。如果近似误差超过了一个临界值，其递归子程序的迭代次数增长非常快。

蒙特卡洛方法是基于统计的方法，该方法能产生复杂网络的近似网络可靠性函数，而不用提前知道所有的最小路集和最小割集。在运行时间和结果准确度方面，该算法都优于同样能产生近似网络可靠度函数的最好算法——线性平方近似法及蒙特卡洛仿真——响应曲面方法。

10.8.3 容量可靠性评估

对于网络连通可靠性的评估是网络可靠性研究中最开始进行的，因此研究成果很多。但在实际使用网络的过程中，会发现网络中不论是链路的容量还是节点的容量，都不是如连通可靠性研究中所默认的“容量无限”。在网络连通的情况下，网络容量的限制依然会对“传输一定流量”的功能实现产生影响。因此，不仅关心网络中是否存在连

通路径，还关心是否存在满足一定流量（物质、能量、信息）需求的连通路径。最早对这一问题进行研究的是美国普林斯顿大学的 Ford 教授等，他于 1956 年针对运输网、通信网、电网等一类容量有限的网络，基于图论提出了网络流模型，并于 1962 年首先给出了求解网络最大流的第一个算法——标号法，其开拓了用数学网络理论来研究运输系统的思路，首次开始将链路容量与网络可靠性相结合。随后，出现了对路网能力可靠性的研究，即将路网能力可靠性定义为路段交通量不超过路段能力限制的概 率口。近年来，才开始对“定量信息通过网络的概率”，即流网络（Flow Network）的研究。

首先对这一问题进行研究的是 K.K.Aggarwal 等人，他们将一个系统是否故障定义为其能否成功地在源汇节点间传输要求的流量。为了简化问题，突出重点，可以做如下假设：

- 网络中的节点无容量限制且完全可靠。
- 网络中的链路有容量限制，不能超出该容量信息流。
- 链路只有故障、正常两种状态，故障时信息流无法通过。
- 网络中链路故障的概率是统计独立的。

传统的网络流理论虽然考虑了网络容量的问题，但都是针对网络容量固定的网络。而现实世界中的网络系统受到多种不确定因素（如网络构件的降级运行、网络阻塞等）的影响，可能会导致网络拓扑结构、链路容量发生变化，从而表现出网络容量的随机性和多态性，所以，使用传统的网络流理论没有考虑到网络容量的这两个特性，用来解决随机环境下的网络实际问题已经不再合适。

因此，近些年来，可靠性工作者们致力于对流网络可靠性评估方法的进一步改善和对随机流网络的研究。

对于流网络的可靠性评估可以使用基于可加性和合格性概念的新算法，它减少了之前的复合路径算法中的冗余计算，从而减少了计算复杂度；也可以使用子集切割技术，其通过枚举所有无冗余的子割集来计算一个大的有异构链路容量的通信网络的可靠性。

对于随机流网络（链路容量为服从已知分布的随机变量的网络）的可靠性评估可以分为容斥原理为基础的精确算法和以上下界法为基础的近似算法。

10.8.4 性能可靠性评估

虽然对于链路容量的可靠性评估方法已经考虑了网络流的负荷问题，但在实际的网络中，保证网络流量的路径并不像考虑链路容量的方法中所假设的那样自动依据拓扑结构生成（有路由算法参与其中），并且网络的拥塞、时延等故障也成为日渐关注的焦点。

网络性能可靠性研究需要解决的主要有以下 3 个难点：

- 如何针对网络的动态性、多态性等特点建立合理的可靠性分析数学模型？
- 基于网络性能的可靠性评估的指标是什么？
- 有哪些方法可以用于网络性能可靠性评估？

性能可靠性的数学模型不再以拓扑信息为中心，而是集中关注于流量路径的信息，通过从流量路径到物理构件和容量的映射，能简单明了地反映网络的性能降级情况，从而能通过一种由上到下的方法评估通信网络的可靠性。

在对网络性能可靠性评估时可以以源信号在规定时间内到达终点的概率为该网络的及时可靠度，以路由缓冲区溢出的概率作为衡量网络拥塞的标准，也可以以接收端数据包接收量与发送端发送量的比例为该网络的完整可靠度。

可以通过外仿真或是内仿真对网络性能可靠性进行评估。对于外仿真，可以假设网络节点完全可靠，链路可靠度为常数，数据包到达时间服从泊松分布，以成功数据包的数量与成功数据包及丢失数据包的数量之和之比作为网络的拥塞可靠度（当存在数据包丢失时），或者将成功数据包数量与仿真产生的所有数据包数量之比作为拥塞可靠度（当没有数据包丢失时）。仿真采用事件驱动方法，考虑 3 种事件：数据包产生、数据包传输、数据包接收。先将时间清单初始化，再按照所有事件发生的时间顺序，将事件添加到事件清单上。

10.8.5 以业务为中心的网络可靠性综合评估

以上三类网络可靠性评估虽然能够反映网络的不同功能要求、度量范围、网络性能，但是很难给出网络运行业务时的综合能力，这就需要对网络的可靠性进行综合评价。对以业务为中心的网络可靠性的综合评估问题可以表述如下：

根据网络中运行的某一项业务实际情况，对于 n ($n>1$) 个网络配置方案 C_1, C_2, \dots, C_n ，构造 m ($m>1$) 个可靠性评价指标 R_1, R_2, \dots, R_m ，通过解析或仿真计算获得各自对应的计算结果 $\{R_{ij}\}$ ，构造评价函数 $y = f(W|R)$ ，使得 C_1, C_2, \dots, C_n 在 $y = f(W|R)$ 的作用下能排出顺序或分为若干类别。其中 $W = (w_1, w_2, \dots, w_m)^T$ ， w_i 为评价指标 R_i 的权重系数 $\left(w_i > 0, \sum_{i=1}^m w_i = 1 \right)$ ， $R = (R_1, R_2, \dots, R_n)^T$ 。

常用的网络可靠性综合评估方法、特点及适用性如表 10-5 所示。

表 10-5 可靠性综合评价方法

类型	名称	特点	适用性
定性评价法	德尔菲法	通过计算大量不同方案各指标间的距离或相似系数，判定指标类别，计算新方案与各类指标间距离或相似系数，判断新方案类别归属	适用于网络可靠性方案归类

(续表)

类型	名称	特点	适用性
线性规划法	数据包络法	以凸分析和线性规划为工具，比较输入、输出间的相对效率，由此得出评价结论	网络可靠性评价不考虑输入，非效率评价，不适用
统计分析法	因子分析法（含主成分分析法）	通过构建因子载荷矩阵，用少数相互独立的公共因子与特殊因子来描述多个相关指标，可简化指标维数。该方法具有客观性、全面性，但新转换出的指标需要专业知识解释	网络可靠性评价都是围绕可靠度这一参数进行的，正交转换出来的参数很难具备物理意义，不适用
	聚类分析与判别分析	通过计算大量不同方案各指标间的距离或相似系数，判定指标类别，计算新方案与各类指标间距离或相似系数，判断新方案类别归属	适用于网络可靠性方案归类
系统工程法	层析分析法	通过把问题表述为有序的递阶层次结构，两两比较确定层次中诸因素的重要性，最后综合成总的重要性排序，适用于方案比较	适用于网络可靠性方案排序
	灰色关联度分析法	一种多因素统计分析方法，用灰色关联度来描述因素间关系的强弱、大小和次序，其实质是利用各方案与最优方案间的关联度大小对评价对象进行比较、排序	适用于可靠性指标为静态值的网络可靠性方案排序
模糊数学法	模糊综合评判法	应用模糊关系合成的原理，从多个因素对被评判事物隶属等级状况进行综合评判，适用于涉及模糊因素的对象系统	适用于可靠性指标为动态值的网络可靠性方案排序
智能方法	人工神经网络法	通过对给定样本模式的学习，获取评价专家的经验、知识、主观判断及对目标重要性的倾向，当需对样本模式以外的对象系统给出综合评价时，可再现评价专家的经验、知识和直觉思维，从而实现定性分析与定量分析的有效结合，既运用了专家智慧，又减少了不确定性	适用于网络可靠性方案归类

10.9

网络可靠性设计

10.9.1

可靠性设计概述

通信网可信性设计需考虑冗余设计、故障管理与预防、数据管理、节点及链路可信性、环境、抗毁能力、安全等因素。应重点考虑以下方面：

- 冗余设计。重点考虑关键设备和链路的冗余。
- 网络保护机制。例如，路由协议、热备份协议、路由绑定协议、自动保护切换协议等都是常用的网络保护机制。
- 容错设计。即进行网络健壮性设计，使之在出现某些错误或故障时，仍能正常工作或部分工作。
- 拥塞控制。通过分析或可信性仿真试验找出网络流量的“瓶颈”，并采取有效的拥塞控制策略。
- 在线维护保障设计。即在不中断网络运行的前提下，实现网络的维护和保障。常用的方法有硬件的热拔插更换和软件的在线升级等。
- 仿真辅助设计。通过网络可信性仿真试验方式，进行网络完成性、抗毁性、可用性、恢复性、可靠性方面的辅助分析和设计。

通信网络冗余设计主要考虑链路冗余、主干设备冗余、供电冗余、服务器冗余4个方面。

系统可靠性设计包括系统冗余设计的总体安排，如冗余传输信道、双磁盘、双主机、数据保护与恢复技术；Cluster（簇）结构等冗余技术的选择与规划；硬件可靠性设计中主要是各种通信设备、计算机及其外围设备生产或选购时的可靠性指标要求；软件特别是网络应用软件的可靠性设计涉及的软件可靠性测试与可靠性增长设计、数据保护与恢复技术、故障诊断与自动校正技术的采用等。除此之外，网络信息系统事实上是一项人机工程，人是网络信息系统应用和运行的主体，因此提高开发方与使用方有关人员的职业道德和技术素质，从心理学和生理学角度来改善和提高人的效能使人机和谐结合，同样是提高网络信息系统可靠性的有效措施。

系统互连与连通性设计包括网络互连设备、互连体系的选择，根据网络的连通度、结合度等指标确定网络的拓扑结构，以及网络连通性故障检测与排除的设计等。

一种简单的链路冗余设计方案，是给主链路增加一条备用链路。以 ISDN 为例，增加另外一条拨号备用线，采用 DDR 的方式，一旦主链路中断，通过拨号 ISDN 就可以启用备用线恢复网络连接。

另一种方法是采用网状或带冗余的星状拓扑结构。

如图 10-13 所示，节点 R_2 和 R_3 需要与中心节点 R_1 通信。方案 1 没有任何冗余设计，当线路 A 或 B 中断时， R_2 或 R_3 无法连接 R_1 。方案 2 和方案 3 有冗余设计，方案 2 为在星型拓扑中的每个非中心节点增加一条到中心节点的冗余链路，方案 3 为网状拓扑。相比较而言，采用网状拓扑的方案 3 显然更有优势：避免中心节点的

瓶颈现象。

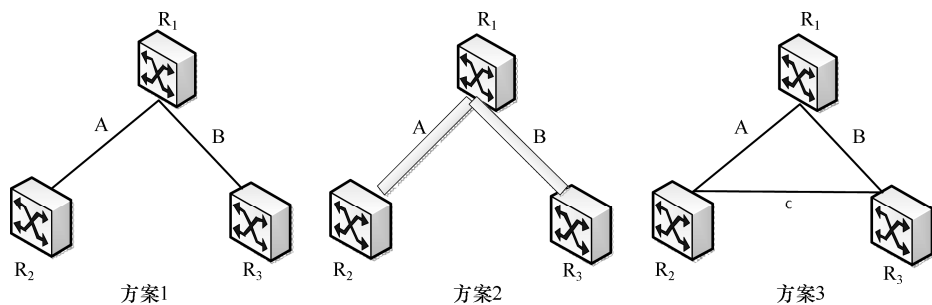


图 10-13 3 种不同网络连接方案

主干设备冗余的典型案例是网络核心交换机的冗余。我们知道，网络核心交换机的故障会导致整个局域网瘫痪，因此，在做较大规模的网络规划时，应采用如图 10-14 所示的双核心交换机热备份结构。采用这种结构可保证任何一个交换机故障时，网络仍能正常工作。

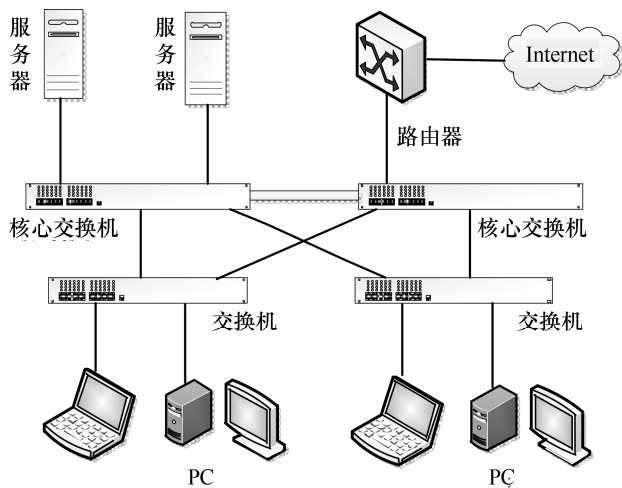


图 10-14 双核心交换机的冗余结构

另一种主干设备冗余的例子是路由器的冗余。路由器的冗余一般通过虚拟路由冗余协议（VRRP）实现，分为两种方式。限于篇幅，在此没有说明其具体实现方法，有兴趣的读者可参考相关文献。

可靠性设计包括网络拓扑设计和业务性能设计，为了提高通信网的可靠性，在设计时采用了各种对策和措施（即可靠性技术）。可靠性设计一直注重物理层的设计，考虑物理网和系统的可靠性。总结国内外的经验，这些措施都是利用了“容错”和“避错”的思想，按照功能上分散和物理上分散的原则采取的，以提高网络

抗灾害和抗过负荷的能力。容错设计的主要方法有：

- 故障限制 (Fault Confinement): 即限制故障的传播范围, 防止故障影响系统的其他部分。
- 故障检测 (Fault Detection): 即尽快发现故障, 减少故障的潜伏期。
- 故障屏蔽 (Fault Masking): 即掩盖故障对输出的影响。
- 重试技术 (Retry Technique): 对故障进行一次或若干次检测, 以消除瞬时故障的影响。
- 故障诊断 (Fault Diagnosis): 检测故障, 并判断故障的位置。
- 重组 (Reconfiguration): 对系统进行重组, 切除故障设备, 换上备份部件。
- 恢复 (Recovery): 检测和重组, 使系统回到故障前的处理点。
- 重新启动 (restart): 当不能消除故障影响时, 采用重新启动的方法重新装载系统, 以期恢复系统的运行。
- 修复 (Repair): 对故障部件进行修理, 使之恢复正常。
- 重构 (Reintegration): 将修复了的部件加入系统, 如果修复是联机进行的, 则重构将不能中断系统的运行。

在实际设计容错系统时, 根据系统的容错性要求, 综合采用上述 10 种容错技术中的若干种技术。

网络容错和避错的主要措施有:

- 同一地区分散设置多个交换中心, 实现负荷分担。
- 传输上实现分散的多手段、多路由组织。
- 为各种设备和系统提供一定的冗余度。
- 强化设备抗灾能力等。

从各种研究来看, 设备和物理网络的可靠性已较高, 设备可靠性在过去十年里每年提高 10%以上。随着网络技术的发展, 特别是宽带网的引入, 可靠性设计已不再局限于此, 人们已开始注重高层的设计技术 (如业务层)。对不同的网络而言, 其设计目标不尽相同, 模拟电话网、数据网和 N-ISDN 的目标是建设一个高可靠性的网络, B-ISDN 和宽带的目标则是要提供具有多种可靠性等级的业务。网络可靠性设计在不同的网络层次上各有侧重, 如在业务层上的流量和拥塞控制、动态路由等; 在逻辑层上的虚拟通路 (VP) 重新分配、自愈等措施; 在物理层上的节点双重备份和路由分散等措施, 并采用高可靠性设备, 以及系统冗余等。

拥塞控制是网络可靠性设计的重要内容。通过限制拥塞扩散和持续时间来减轻拥塞的一组操作。拥塞控制的作用见图 10-15。

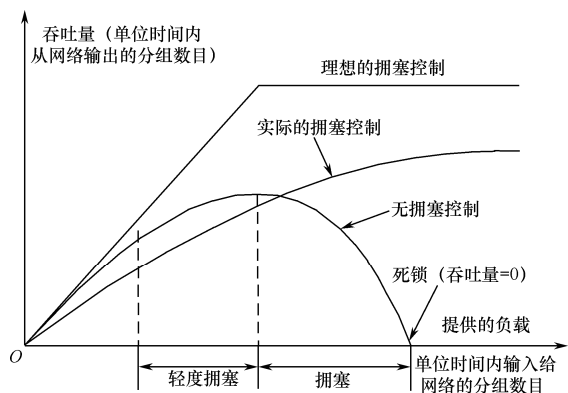


图 10-15 拥塞控制示意图

可从增加网络资源和降低用户需求两方面解决拥塞问题。前者一般通过动态配置网络资源来提高系统容量，如在高峰时增加接入线路，在卫星链路上增加发射功率来提高可用带宽，通过路径分裂（path splitting）用多条不同的物理路径来满足用户需求等。

降低用户需求主要表现在以下 3 方面：

- 拒绝服务：在拥塞发生时，拒绝接纳新的用户请求。例如，电话网中的忙音。
- 降低服务质量：所有用户（包括新用户）在拥塞时降低其发送速率。例如，分组交换中的滑窗算法等。
- 调度：合理安排用户对网络资源的使用，保证总需求永远小于网络可用资源。例如轮循、优先级设定、资源预留等。

可根据拥塞时间的长短或拥塞发生频度确定选用何种拥塞控制机制，见图 10-16。对频繁发生拥塞的网络，最好的办法是重新规划和设计以匹配需求的模式；对偶发的适度拥塞连接接纳控制（CAC）是一种有效措施；对拥塞时间小于连接持续时间的情形，端-端反馈策略是可行的。

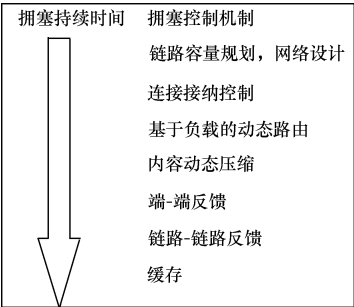


图 10-16 拥塞持续时间与拥塞控制机制的关系

在网络不同层次, 拥塞控制策略主要有:

- 传输层: 重传策略、乱序缓存策略、确认策略、流控制策略和确定超时策略。
- 网络层: 子网内部的虚电路与数据报策略、分组排队和服务策略、分组丢弃策略、路由算法和分组生存管理。
- 数据链路层: 重传策略、乱序缓存策略、确认策略和流控制策略。

通信网可靠性研究的根本目的就是消除造成网络可靠性下降的各种故障和拥塞, 提高网络运行质量, 更好地满足社会和用户的通信需求。目前国外一些组织机构在可靠性方面的研究结果已被一些电信运营公司所采用。例如: 日本所制定的“稳定基准”, 对于设备发生不可预知的故障或过负荷等异常使用状态时应确保的接续、传输质量及其可靠性给出了规定, 并对接续系统一般故障和异常故障时的稳定质量要求进行了分配。Bellcore 则对交换系统、传输系统、宽带交换系统, 以及光纤传输系统的可靠性进行了专门研究, 除了对硬件可靠性的研究应用外, 近年来还加强了软件可靠性的研究应用, 如快速自动恢复系统, 采用后使网络的可靠性明显提高, 故障平均恢复时间从采用系统前的 15 小时降到了采用后的 5 分钟, 全网的阻塞次数从全年 7 亿次降到了 18 万次。

10.9.2 通信网可靠性设计准则

制定通信网的可靠性设计准则时, 应重点考虑以下方面:

① 抗毁性设计, 主要包括:

- 对通信设施进行物理加固, 提高其抗毁性, 从而提高通信网系统的抗毁性。
- 增加关键网元的冗余度, 进行基于网络拓扑的链路冗余设计, 包括采用增加设备备份, 采用多种传输手段, 多频段工作等措施, 保证关键网元和链路的可靠性。
- 建立最低必要应急通信网, 即建立具有极强抗毁能力的核心小容量网络, 以维持最少、最必要的通信。
- 采用抗电子战能力强的通信技术或受电子战影响小的通信方式, 如抗频通信技术等。
- 采用模块式结构, 使模块具有检测、报告自身故障的能力。进行可重构设计, 使模块在遭到破坏的情况下, 系统能快速实现功能重构。
- 疏散目标大的设备, 提高设备机动能力, 缩短架设时间和开通时间。
- 进行网络互通性设计, 提高网络内部用户之间的互通能力, 以及与其他网络用户的通信能力。
- 通过分析、仿真等手段找出网络的薄弱环节, 进行优化设计, 减少或消除薄



弱环节，如：对网络拓扑进行分布式设计，以防止通信网中控制功能集中，部分被毁导致全网瘫痪。

② 进行故障管理设计，建立故障探测、故障诊断、故障隔离、故障恢复、故障移出、故障告警、故障预测及预防机制。设计要点如下：

- 故障检测：监视网元和链路的工作状态，设置网络各种性能的阈值，监视网络性能变化情况，以及时发现故障。
- 故障诊断：故障发生时，根据收集到的信息数据准确定位故障发生的位置和原因。对于不能直接定位的故障，可以根据故障信息的关联关系分析确定故障具体发生的位置和原因。
- 故障隔离：隔离故障部件，防止其对网络其他部件的影响。
- 故障恢复：故障发生后利用复位部件或部分部件重启等方法恢复网络业务，对于具有冗余设计的单元，采用保护倒换或重新分配资源等技术，以避免网络业务故障。
- 故障移除：借助维修保障体系，对故障的部件进行更换，包括事后的进一步深层分析，以对整网的解决方案提出改善措施。
- 故障告警：网络故障发生后，相关单元及时上报告警给网络管理系统，可以针对不同的故障等级提供不同的报警手段。网络管理系统收集相关故障告警信息用于故障定位及后期的进一步分析。
- 故障预测及预防：利用趋势图，多变量综合分析等方法分析评估故障发生的概率和时机，采取预防措施。

③ 进行数据管理设计，采用定期备份、镜像技术、加密技术、重要数据冗余等技术，保证网络数据的可靠性和安全性。

④ 充分考虑环境对网络可信性的影响，进行耐环境设计。

⑤ 通过路由协议、自动倒换保护协议、热备份协议等建立网络保护机制。

⑥ 通过分析找到网络流量的“瓶颈”，采取有效措施实现拥塞控制。

⑦ 按 GJB/Z 102 对通信软件进行可靠性、安全性设计。

⑧ 建立针对通信网硬件、软件、固件、人员操作故障的应对策略。

⑨ 进行网络人员操作防差错设计，减少人员误操作和操作流程错误对网络可信性的影响。

10.10 网络可靠性管理

参照一般可靠性管理的内容，我们就可大体确定网络运营者在各阶段的可靠性

管理内容，如表 10-6 所示。

表 10-6 各阶段网络可靠性管理的内容

阶段	内容
方案论证阶段	确定网络可靠性要求和计划 确定网络可靠性工作项目
分析设计阶段	提出网络设计的可靠性标准、规范 提出某一网络系统的可靠性设计水平 提出对设备的固有可靠性要求 网络可靠性规划的经济分析 分析并确定网络组织中的各种可靠性措施
建设实施阶段	组织和实现各种可靠性措施及保障措施 对建设结果进行监督和评价 对建设部分进行试验和鉴定
运行维护阶段	分析、评价网络运行的可靠性水平 制定网络维护、管理的体制和规程 制定维护、管理的任务、要求和措施 分析各种故障规律，提出相应的可靠性措施 规划可靠性增长目标，并进行控制 对重大异常故障，制定应急通信制度和措施 监督各种制度和措施的执行

首先，在方案论证阶段，应确定网络可靠性的定性和定量要求，制订可靠性工作计划，并明确拟开展的可靠性工作项目。

在分析设计阶段，企业需要了解如何评价一个网络的固有可靠性；如何将网络可靠性分配到各系统和设备；有哪些措施可以提高网络的可靠性；对设备和系统有什么要求等。对这些问题的组织和决策就构成了分析阶段的可靠性管理。

在网络的建设实施阶段，企业已经有了关于网络及其可靠性的设计方案。这个阶段就是要从物理上实现这个可靠性方案，如电路冗余度、不同传输路由的设置、物理设施的分散配置、机房条件的保证等。为了保证实施的质量，就离不开可靠性管理的监督和建设完成后的试验、验收和评价。

对于网络来说，运行维护阶段的管理更为重要。随着网络技术的发展和在网络可靠性的研究，已经有很多技术和措施可以用来设计一个可靠的网络。但网络运行可靠与否，能否完成实际运行中用户的功能要求，只有在运行中才能验证，各种各样的可靠性问题也是在运行中暴露出来的。因此，我们需要对网络运行的可靠性（广义的工作可靠性）进行评价、分析。为了预防或解决网络运行中不时出现的各种问题，需要建立相应的制度和工作要求，需要对网络可靠性增长进行规划和控制



等等。这些工作就构成了运行维护阶段的可靠性管理内容。

上述分析是一种静态的观点。其实,因为管理的环境和各种要素都是动态变化的,管理本身是动态的,这要求网络可靠性的管理也应是动态的。比如,在网络的不同发展时期管理的重点可能是不同的,在各个阶段可能会有一些临时性问题需要现场决策,而且,网络可靠性的管理要适应网络技术和用户需求的变化等等。

当然在网络可靠性管理中,还有两个可靠性管理的基础内容:信息管理和人员管理。为了对网络的可靠性进行分析和评价,掌握网络运行中的故障规律等,需要有大量的网络运行数据为依据,这就离不开运行数据库的建设和信息管理。同时每一项工作都是由人来参与的,工作完成质量的好坏在一定程度上取决于工作人员的工作态度和业务素质。

10.11

小结

本章首先介绍了网络可靠性研究中的一些基本概念,如网络的概念,网络的发展,网络的特征量,不同分类标准下网络的分类情况。随后,从网络故障的来源和网络故障的分类两个方面分别概述了网络故障的相关情况,并以计算机网络为例,从故障模式和故障原因两个角度分析了网络中各类故障所占的百分比,为后续网络可靠性的分析奠定一定的基础。

本章重点阐述了目前网络可靠性的研究方法和成果,给出了网络可靠性的定义,并对定义中的关键词做出了详细的解释;总结了网络可靠性研究中涉及的主要理论方法;根据实际情况,总结了网络可靠性研究中参数体系的建立原则,给出了网络可靠性的通用参数体系和通信网络可信性研究中的参数体系;从网络可靠性建模的实施要点和网络可靠性模型的分类两个方面概述了网络可靠性建模的相关问题;总结分析了网络可靠性解析算法、网络可靠性仿真算法,并比较了各类可靠性计算方法的优缺点,并以两个网络为例,进行了仿真计算案例分析;在确定网络可靠性研究框架的基础上,将网络可靠性评估分为了连通可靠性评估、容量可靠性评估、性能可靠性评估和以业务为中心的网络可靠性综合评估,并分别进行了概述;根据网络特点,对网络可靠性的设计进行了概述,给出网络可靠性设计的准则;最后,根据网络层次划分和网络所处阶段,对网络可靠性管理的研究内容和管理内容进行了阐述。

参考文献

- [1] 周海平. 复杂网络的演化模型及传播动力学模型研究, 贵州大学博士学位论

文, 2009.

- [2] Erdős P, Rényi A. On random graphs, publications Mathematic, 1959, 6: 290~297.
- [3] 欧拉 (Leonard Euler, 1707-1783) 简况: <http://www2.zzu.edu.cn/math/classes/2003/yl/oula.htm>.
- [4] Erdős P, Rényi A. On the Evolution of Random Graphs, Pub. Math. Inst. Hung. Acad. Sci., 1959, 5: 17~60.
- [5] Erdős P, Rényi A. On the strength of connectedness of a random graph, Acta Mathematica Scientia Hungary, 1961, 12: 261~267.
- [6] Watts D J, Strgatz Steven H. Collective dynamics of “small-world” networks. Nature, 1998, 393 (6684): 440~442.
- [7] Migram S. The small world problem. Psychology Today, 1967, 1: 61~67.
- [8] Dodds P S, Muhamad R, Watts D J. an experimental study of search in a global social networks. Science, 2003, 301 (5634): 827~829.
- [9] 汪小帆, 李翔, 陈关荣. 复杂网络理论及其应用. 北京: 清华大学出版社, 2006.
- [10] Albert R, Jeong H, Barabási A L, Error and attack tolerance of complex networks. London: .Nature. 2000, 406: 378~382.
- [11] Barabási A L, Jeong H, Ravasz E. Evolution of the social network of scientific collaborations. Physica A, 2004, 311: 590~614.
- [12] 张俊良. 复杂网络可靠性研究. 大连理工大学硕士学位论文, 2006.
- [13] Newman MEJ. The Structure and Function of Complex Networks. SIAM Review (S0036-1445), 2003, 45 (2): 167~256.
- [14] Jeong H., Mason S. P., Barabasi A. L., et al. Lethality and centrality in protein networks. Nature, 2001, 411 (6833): 41~42.
- [15] Guimer R., Amaral L. Modeling the world-wide airport network. The European Physical Journal B - Condensed Matter, 2004, 38 (2): 381~385.
- [16] 张宇栋. 基于复杂系统理论的连锁故障大停电研究. 浙江大学博士学位论文, 2013.
- [17] Duncan J. Watts. The “New” Science of Networks. Annual. Review of Sociology, 2004, 30: 241~270.
- [18] O.Wing and P.Demetriou. Analysis of Probabilistic Networks. IEEE Transactions on Communications Technology, 1964, 12 (3): 38~40.
- [19] L.Fratta and U.G.Montanari. A Recursive Method Based on Case Analysis for Computing Network Terminal Reliability. IEEE Transactions on



Communications Technology, 1978, 26 (8): 1166~1177.

- [20] 吴东海, 周鸿志. 军用通信网系统可靠性研究与应用. 中国国防科技报告 (总参通信部军事代表局), 2010.
- [21] Weiyi Zhao, Jiang Xie. OPNET-based modeling and simulation study on handoffs in Internet-based infrastructure wireless mesh networks. Computer Networks, 2011, 55: 2675~2688.
- [22] 叶酉荪, 南庚. 军事通信网分析与系统集成. 北京: 国防工业出版社, 2005.
- [23] 陈敏. OPNET 网络仿真. 北京: 清华大学出版社, 2004.
- [24] 张铭, 窦赫蕾, 常春藤. OPNET Modeler 与网络仿真. 北京: 人民邮电出版社, 2007.
- [25] 袁崇义. Petri 网原理. 北京: 电子工业出版社, 1998.
- [26] 原菊梅. 复杂系统可靠性 Petri 网建模及其性能分析方法. 北京: 国防工业出版社, 2011.
- [27] 杨为民, 阮镰, 俞沼, 等. 可靠性维修性保障性总论. 北京: 国防科技工业出版社, 1995.
- [28] Yang W M, Ruan L, Tu Q C. Reliability System Engineering Theory and Practice, In Proceedings of the Second International Conference on Reliability, Maintainability and Safety. Beijing: Chinese Society of Aeronautics and Astronautics, 1994, 7~10.
- [29] 张学渊, 梁雄健. 关于通信网可靠性定义的探讨. 北京邮电大学学报, 1997, 20 (2): 30~35.
- [30] 杨为民, 等. 系统可靠性数字仿真. 北京: 北京航空航天大学出版社, 1990.
- [31] 杨宇航, 冯允成. 基于仿真的复杂系统可靠性、可用性和 MTBF 评估文献综述. 系统工程理论与实践, 2003. 2: 80~85.
- [32] 方再根. 计算机模拟和蒙特卡洛方法. 北京: 北京工业学院出版社, 1988.
- [33] 肖刚, 李天柁. 系统可靠性分析中的蒙特卡洛方法. 北京: 科学出版社, 2003.
- [34] 国防科技大学 C3I 研究中心. 基于对象的 Petri 网建模仿真环境 OPMSE. 技术报告, 1999.
- [35] 张磊, 向德全. 模糊 Petri 网在军用信息系统效能分析中的应用. 海军工程大学学报, 2007, 19 (6): 125~128.
- [36] 罗雪山, 张维明. C3I 系统理论基础—C3I 系统建模方法与技术. 长沙: 国防科技大学出版社, 2000.

- [37] 吴东海. 军用通信网系统可靠性评估及其仿真方法研究. 电子科技大学硕士学位论文, 2012.
- [38] 方锦清, 汪小帆, 郑志刚, 毕桥, 狄增如, 李翔. 一门崭新的交叉科学: 网络科学(上). 物理学进展, 2007, 27(3): 239~341.
- [39] 杨娇. 二分图网络故障传播模型与故障诊断算法研究. 东北大学硕士学位论文, 2010.
- [40] 刘康平, 李增智. 网络告警知识发现研究与实现. 计算机工程与应用, 2001, 37(23): 25~27.
- [41] 史铁林. 层次分类诊断模型. 华中理工大学学报, 1993, 21(1): 6~11.
- [42] 李瑞莹. 网络可靠性评价方法研究. 北京航空航天大学博士学位论文, 2006.
- [43] 黄宁. 网络可靠性研究现状与发展趋势. 可靠性工程, 2012, 3: 130~137.
- [44] 赵娟, 郭平, 邓宏钟, 吴俊, 谭跃进, 李建平. 基于信息流动力学的通信网络性能可靠性建模与分析. 通信学报, 2011, 32(8): 159~164.
- [45] 匡罗贝, 肖晓强, 李皓平, 胡华平. 一种自相似网络可靠性分析模型. 计算机工程与应用, 2007, 43(24): 134~137.
- [46] Buzna L, Peters K, Helbing D. Modelling the dynamics of disaster spreading in networks. *Physica A: Statistical Mechanics and its Applications*, 2006, 363(1): 132~140.
- [47] Buzna L, Peters K, Ammoser H, et al. Efficient response to cascading disaster spreading. *Physical Review E*, 2007, 75(5): 056107.
- [48] 翁文国, 倪顺江, 申世飞, 等. 复杂网络上灾害蔓延动力学研究. 物理学报, 2007, 56(4): 1938~1943.
- [49] 郭天柱. 复杂网络中心性及其对灾害传播影响的研究. 大连理工大学硕士学位论文, 2009.
- [50] 李泽荃, 张瑞新, 杨翌, 等. 复杂网络中心性对灾害蔓延的影响. 物理学报, 2012, 61(23): 238902~238902.
- [51] Jinyong Huang, Yong Pan. Simulating Test For Communication Network Dependability Design and Verification. In *Proceedings of the 10th International Conference on Reliability, Maintainability and Safety*, Aug. 2014.
- [52] 林闯, 单志广, 任丰原. 计算机网络的服务质量(QoS). 北京: 清华大学出版社, 2004.
- [53] 梁雄健, 孙青华, 等. 通信网可靠性管理. 北京: 北京邮电大学出版社, 2004.

第11章

可靠性标准

11.1 概述

可靠性标准是可靠性工程技术与管理的重要基础之一，是指导开展各项可靠性工作使其规范化、最优化的依据和保证。吸收、引进可靠性国际先进标准是迅速提高我国可靠性工程技术与管理水平的重要途径。可靠性标准是在严密的理论指导下通过总结工程与管理的实践经验而制定的，随着理论研究、工程技术的发展和经验的积累，可靠性标准不断修订补充和完善，有高度的科学性、实用性和指令（或指导）性。

可靠性标准体系分三个层次，即：可靠性基础标准、专业可靠性基础标准、有可靠性要求的产品标准。可靠性基础标准是指对可靠性工程技术与管理有广泛指导意义的基础标准；专业可靠性基础标准是指某一大类产品公用的可靠性标准；有可靠性要求的产品标准是指各种有可靠性指标要求的具体产品标准。可靠性标准按级别分为国家可靠性标准（GB）、国家军用可靠性标准（GJB）、部委可靠性专业标准、企业可靠性标准。按内容分为管理、采购、研制、生产、试验、分析、安装、储运、使用、维修等各个方面的标准。按形式分为规范、标准、手册等。

我国标准化部门、标准化及可靠性工作者多年来在引进、消化国外可靠性标准的基础上，制定了我国的可靠性标准，先后发布了一系列有关可靠性名词术语、产品、技术、程序、方法和管理等方面的标准，逐步形成可靠性领域的标准体系。截止到2012年底，我国已发布的可靠性标准，包括GB/T、GJB、JB/T、SJ/T、QC/T等方面能够查到的各类可靠性标准共有403项，其中，可靠性通用技术标准共30项，仅占总数的7.5%。美国截止到2012年7月共有539项可靠性标准（包括美国军标和各协会标准），其中通用技术标准76项（包括通用技术要求、通用方法、名词术语等）约占14%。其他如德国、日本、英国在其可靠性标准中通用技术标准都占较大比例。因此，应加强我国可靠性通用技术标准的制定力度，提高通用标准的比重。

11.2 可靠性国际标准

11.2.1 可靠性国际标准组织

国际标准是指国际标准化组织（International Organization for Standardization, ISO）、国际电工委员会（International Electrotechnical Commission, IEC）和国际电信联盟（International Telecommunication Union, ITU）制定的标准，以及国际标准化组织确认并公布的其他国际组织制定的标准。国际标准在世界范围内统一使用。

目前参与制定可靠性国际规范和标准的组织主要有：美国航空与航天局（National Aeronautics and Space Administration, NASA）、北大西洋公约组织（North Atlantic Treaty Organization, NATO）、英国标准协会（British Standards Institute, BSI）、英国国防部（Ministry of Defence, MOD）、美国国家标准协会（American National Standards Institute, ANSI）、加拿大标准协会（Canadian Standards Association, CSA）、电器和电子工程师协会（Institute of Electrical and Electronics Engineers, IEEE）、电子线路连接与包装学会（Institute of Printed Circuits, IPC）、国际电工委员会、国际自动化工程师协会（Society of Automotive Engineers, SAE）、环境科学学会、国际标准化组织、电子工业协会（Electronic Industries Association, EIA）。

11.2.2 IEC 制定的可靠性标准

1. IEC 概况

可靠性标准进入国际标准领域是在 1965 年。当时在美国的建议下，根据可靠性和标准化发展需要，国际电工委员会（IEC）决定成立一个名为“电子元件和设备可靠性”的技术委员会（即 TC 56）。随着可靠性工程技术的不断拓展，维修性和维修保障性的相继提出，该技术委员会的名称也跟着不断发生改变。1973 年起 TC 56 更名为“可靠性与维修性技术委员会”。1991 年起又更名为“可信性”（Dependability）技术委员会，此名称一直沿用至今。早年 TC 56 标准的制/修订工作，是采用成立标准编制工作组的方式进行。编制任务完成后，该标准工作组自行解散。随着 IT 产业的高速发展，软件和网络及系统方面的可靠性问题已日益受到工程界的普遍关注，与之相应的技术与管理方面的标准需求也不断上升，因此根据可靠性标准发展的需求，TC 56 不仅对整个可靠性标准体系进行了大的调整，而且也

对上述标准编制的组织方式进行了改革。为了使工作组的工作具有系统性与连贯性, TC 56 将工作组按专业合并为 4 个大工作组 (Working Group), 即: 可信性名词术语工作组 (WG1)、可信性技术工作组 (WG2)、可信性管理工作组 (WG3) 和系统可信性工作组 (WG4)。然后, 再根据标准制/修订任务和专业分工的需求, 在各个工作组下成立临时标准工作项目小组 (Project Team)、维护小组 (Maintenance Team) 和咨询小组 (Advisory Groups)。

我国的可靠性标准化工作起步于 20 世纪 70 年代初。“全国电工电子产品可靠性与维修性标准化技术委员”(即“可标委”)成立于 1982 年, 挂靠在工业和信息化部电子第五研究所(原来的信息产业部电子第五研究所), 是我国与 IEC/TC 56 对口的专业技术标准化组织。原由国家技术监督局管理, 现归国家标准化管理委员会管理。从 20 世纪 80 年代起, “可标委”跟踪和参与了 IEC/TC 56 国际标准的制定与修订工作, 承担了多项可靠性与维修性领域的国家标准制定任务。

2. IEC/TC 56 的标准体系

早年的可靠性标准没有完整的体系。当时除了有 IEC-605 “设备可靠性试验”和 IEC-706 “设备维修性指南”两大系列标准外, 其他标准基本上是成熟一个就制定一个, 无所谓标准的体系与层次。随着可靠性技术的不断拓展和可信性工程概念的建立, 为满足工程技术发展的需要, TC 56 在 1987 年提出了可靠性标准的“工具箱”结构概念, 并以此作为可靠性标准体系的基础。

IEC TC 56 的标准体系架构如图 11-1 所示, 分为 4 个层次, 即:

- 核心标准: 提供可信性顶层管理、框架方面的指引方面的标准。
- 过程标准: 可信性项目、可靠性、可用性、维修性、保障性和系统可靠性方面的应用过程标准。
- 支撑标准: 可信性试验、统计、预计、建模、保证方面的方法和工具标准。
- 辅助标准: 其他辅助标准。

另外, 在国际标准的编号方面, IEC 经与国际标准化组织 (ISO) 协调后决定: ISO 对其发布的标准使用 60 000 以下的序列编号, 而 IEC 则使用 60 000 以上的编号。因此, 从 1997 年 1 月开始, IEC/TC 56 对其发布的标准, 在原编号基础上都增加了 60 000。例如, 将原来的 IEC 605 变成 IEC 60 605; IEC 706 变成了 IEC 60 706 等, 其技术内容不变。而采用工具箱概念后, 就意味着 TC 56 标准的编号, 将以 IEC 60 300 为核心分为 4 个层次编排。因此, 它除了是一种编号系统外, 这种编排方法也为 TC 56 标准的编制计划、新工作项目的必要性认证、工作任务和资源的分配提供了帮助。由于受原有的但仍然有效的旧标准编号影响, 工具箱的标准编号是独立的, 一些原有旧的“随机”编号将继续使用。另外, 有经验的人员也可以

不借助“应用指南”的帮助，直接使用工具箱的标准。

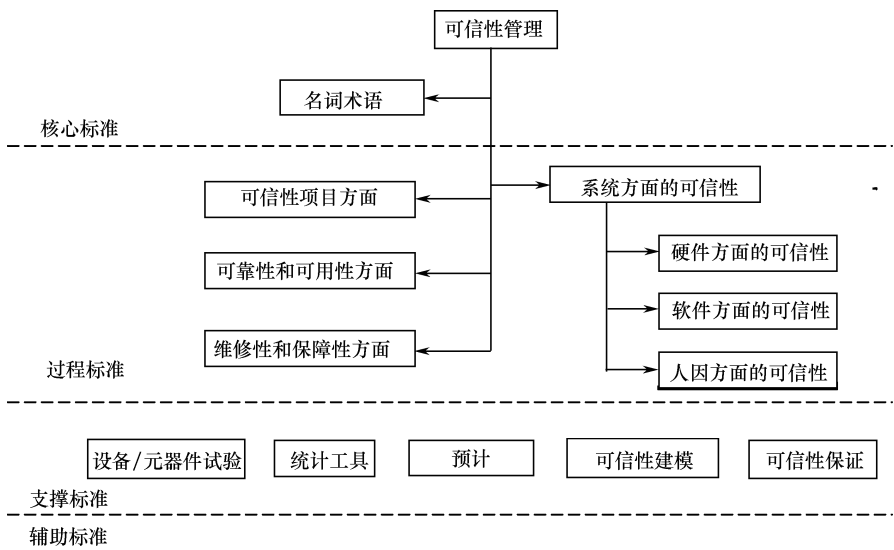


图 11-1 IEC 的可靠性标准体系

IEC 的一些可靠性国际标准的相关信息如表 11-1 所示。

表 11-1 IEC 制定的国际可靠性标准

标准类型	标准编号	标准名称
基础通用标准	IEC 60050-192:2015	International electrotechnical vocabulary –Part 192: Dependability 国际电工词汇——第 192 部分：可信性
	IEC 60300-1-2003	Dependability management - Part 1: Dependability management systems 可信性管理——第 1 部分：可信性管理系统
	IEC 60300-2-2004	Dependability management - Part 2: Guidelines for dependability management 可信性管理——第 2 部分：可信性大纲要素和任务
	IEC 60300-3-1-2003	Dependability management - Part 3-1: Application guide - Analysis techniques for dependability - Guide on methodology 可信性管理——第 3 部分：应用指南——第 1 节：可靠性技术分析——方法学指南
	IEC 60300-3-2-2004	Dependability management - Part 3-2: Application guide - Collection of dependability data from the field 可信性管理——第 3 部分：应用指南——第 2 节：可信性数据的收集
	IEC 60300-3-3-2005	Dependability management - Part 3-3: Application guide - Life cycle costing 可信性管理——第 3 部分：应用指南——第 3-3 节：寿命周期费用分析
	IEC 60300-3-4-2007	Dependability management - Part 3-4: Application guide - Guide to the specification of dependability requirements 可信性管理——第 3 部分：应用指南——第 4 节：可信性要求规范指南



(续表)

标准类型	标准编号	标准名称
基础通用标准	IEC 60300-3-5-2001	Dependability management - Part 3-5: Application guide - Reliability test conditions and statistical test principles 可信性管理——第 3-5 部分：应用指南——可靠性试验条件和统计试验原则
	IEC 60300-3-7-1999	Dependability management - Part 3-7: Application guide - Reliability stress screening of electronic hardware 可靠性管理——第 3-7 部分：应用指南——电子硬件可靠性压力扫描
	IEC 60300-3-9-1995	Dependability management - Part 3: Application guide - Section 9: Risk analysis of technological systems 可靠性管理——第 3 部分：应用指南——第 9 节：技术设备的磁盘分析
	IEC 60300-3-10-2001	Dependability management - Part 3-10: Application guide - Maintainability 可信性管理——第 3-10 部分：应用指南——维修性
	IEC 60300-3-11-2009	Dependability management - Part 3-11: Application guide - Reliability centred maintenance 可信性管理——第 3-11 部分：应用指南——以可靠性为中心的维修
	IEC 60300-3-12-2011	Dependability management - Part 3-12: Application guide - Integrated logistic support 可信性管理——第 3-12 部分：应用指南——综合后勤保障
	IEC 60300-3-15-2009	Dependability management - Part 3-15: Application guide - Engineering of system dependability 可信性管理——第 3-15 部分：应用指南——系统可靠性工程
	IEC 60300-3-16-2008	Dependability management - Part 3-16: Application guide - Guidelines for specification of maintenance support services 可靠性管理——第 3-16 部分：应用指南——维护支持服务的规范指南
	IEC 62347-2006	Guidance on system dependability specifications. 系统可靠性规范指南
	IEC 61650-1997	Reliability data analysis techniques - Procedures for comparison of two constant failure rates and two constant failure (event) intensities 可靠性数据分析技术——两种恒定故障率和两种恒定故障（元素）强度的比较程序
	IEC 61703-2001	Mathematical expressions for reliability, availability, maintainability and maintenance support terms 可靠性、有效性、维修性和维修支持术语的数学表示

(续表)

标准类型	标准编号	标准名称
基础通用标准	IEC 61907-2009	Communication network dependability engineering 通信网络可信性工程
	IEC 62429-2007	Reliability growth - Stress testing for early failures in unique complex systems 可靠性增长——单一复杂系统早期失效的应力测试
	IEC 62502-2010	Analysis techniques for dependability - Event tree analysis (ETA) 可靠性分析技术——事件树分析 (ETA)
	IEC 62508-2010	Guidance on human aspects of dependability 人因可信性指南
	IEC 62551-2012	Analysis techniques for dependability - Petri net techniques 可信性分析技术——Petri 网技术
	IEC 62628-2012	Guidance on software aspects of dependability 软件可信性指南
	IEC/PAS 62814-2012	Dependability of software products containing reusable components - Guidance for functionality and tests 含重用元件的软件产品可靠性——功能性和试验导则
	IEC 60605-2-1994	Equipment reliability testing - Part 2: Design of test cycles 设备可靠性试验——第2部分：试验周期的设计
	IEC 60812-2006	Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA) 系统可靠性分析技术——失效模式和效应分析 (FMEA) 程序
	IEC 61014-2003	Programmes for reliability growth 可靠性增长程序
	IEC 61123-1991	Reliability testing - Compliance test plans for success ratio 可靠性试验——成功率用性能审核试验计划
	IEC 61124-2012	Reliability testing - Compliance tests for constant failure rate and constant failure intensity 可靠性试验——恒定故障率和恒定故障强度的审核试验
	IEC 61163-1-2006	Reliability stress screening - Part 1: Repairable assemblies manufactured in lots 应力筛分的可靠性——分组制造零件的可维修性
	IEC 61163-2-1998	Reliability stress screening - Part 2: Electronic components 应力筛分的可靠性——第2部分：电子元件

IEC 62211-2003	Inductive components - Reliability management 电感元件——可靠性管理
IEC/TS 61586-1997	Estimation of the reliability of electrical connectors 电气接触点可靠度的评估



(续表)

标准类型	标准编号	标准名称
产品标准	IEC 61709-2011	Electric components – Reliability – Reference conditions for failure rates and stress models for conversion 电子元器件——可靠性——失效率 and 应力模型转换的参考条件
产品标准	IEC 61747-5-3-2009	Liquid crystal display devices - Part 5-3: Environmental, endurance and mechanical test methods - Glass strength and reliability 液晶显示装置——第 5-3 部分：环境、耐久性和机械试验方法——玻璃强度和可靠性
	IEC/TR 62059-11-2002	Electricity metering equipment - Dependability - Part 11: General concepts 电量计量设备——可靠性——第 11 部分：一般概念
	IEC/TR 62059-21-2002	Electricity metering equipment - Dependability - Part 21: Collection of meter dependability data from the field 电量测量设备——可靠性——第 21 部分：测量可靠性数据的现场收集
	IEC 62059-32-1-2011	Electricity metering equipment - Dependability - Part 32-1: Durability - Testing of the stability of metrological characteristics by applying elevated temperature 电测量设备——可靠性——第 32-1 部分：耐久性——用于高温下的计量特性稳定性测试
	IEC 62059-41-2006	Electricity metering equipment - Dependability - Part 41: Reliability prediction 电计量设备——可靠性——第 41 部分：可靠性预计
	IEC 62309-2004	Dependability of products containing reused parts - Requirements for functionality and tests 含再用部件的产品的可靠性——功能性要求和试验
	IEC PAS 62326-14-2010	Printed boards Part 14: Device embedded substrate .Termino logy/reliability/design guide 印刷电路板——第 14 部分：设备嵌入式基底——术语/可靠性/设计指南
	IEC 60319-1999	Presentation and specification of reliability data for electronic components 电子元器件可靠性数据的表示和规范
	IEC 61086-3-1-2004	Coatings for loaded printed wire boards (conformal coatings) - Part 3-1: Specifications for individual materials - Coatings for general purpose (Class 1), high reliability (Class 2) and aerospace (Class 3) 加感印制电路板用涂覆层（保形敷层）——第 3-1 部分：专用材料规范——活页 1：通用（I 类）和高可靠性（II 类）涂层
	IEC 61751-1998	Laser modules used for telecommunication - Reliability assessment 电信用激光模量——可靠性评定

(续表)

标准类型	标准编号	标准名称
产品标准	IEC 61810-2-2011	Electromechanical elementary relays - Part 2: Reliability 机电式非定时限有或无继电器——第2部分：可靠性
	IEC 61810-2-1-2011	Electromechanical elementary relays - Part 2-1: Reliability - Procedure for the verification of B10 values 机电式初级继电器——第2-1部分：可靠性——B10值的确认规程
	IEC 62005-9-2-2007	Reliability of fibre optic interconnecting devices and passive optical components - Part 9-2: Reliability qualification for single fibre optic connector sets - Single mode 光纤互连装置和无源部件的可靠性——第9-2部分：单模光纤连接器装置的可靠性鉴定——单模
	IEC/TR 62048-2011	Optical fibres - Reliability - Power law theory 光纤——可靠性——幂律理论
	IEC 62059-31-1-2008	Electricity metering equipment - Dependability - Part 31-1: Accelerated reliability testing - Elevated temperature and humidity 电计量设备——可靠性——第31-1部分：可靠性加速测试——高温和潮湿
	IEC 62005-1-2001	Reliability of fibre optic interconnecting devices and passive components - Part 1: Introductory guide and definitions 光纤互连装置和无源部件的可靠性——第1部分：介绍性指南和定义
	IEC 62005-2-2001	Reliability of fibre optic interconnecting devices and passive components - Part 2: Quantitative assessment of reliability based on accelerated ageing test - Temperature and humidity; steady state 光纤互连装置和无源部件的可靠性——第2部分：基于加速老化试验的可靠性的定量评定——温度和湿度；稳态
	IEC 62005-3-2001	Reliability of fibre optic interconnecting devices and passive components - Part 3: Relevant tests for evaluating failure modes and failure mechanisms for passive components 光纤互连装置和无源部件的可靠性——第3部分：无源部件的故障模式和故障机理评价的相关试验
	IEC 62005-7-2004	Reliability of fibre optic interconnecting devices and passive optical components - Part 7: Life stress modeling 光纤互连装置和无源部件的可靠性——第7部分：寿命应力模型
	IEC/TR 62572-2-2008	Fibre optic active components and devices - Reliability standards - Part 2: Laser module degradation 光纤有源元件和器件——可靠性标准——第2部分：激光模块的衰变



(续表)

标准类型	标准编号	标准名称
产品标准	IEC 62572-3-2011	Fibre optic active components and devices - Reliability standards - Part 3: Laser modules used for telecommunication 光纤有源元件和器件——可靠性标准——第 3 部分: 电信用激光模块
	IEC/TR 62627-03-01-2011	Fibre optic interconnecting devices and passive components - Part 03-01: Reliability - Design of an acceptance test for fibrepistoning failure of connectors during temperature and humidity cycling: demarcation analysis 光纤互连设备和无源元件——第 03-01 部分: 可靠性——温度和湿度循环器件连接器的纤维活塞故障用验收试验的设计: 界限分析
	IEC/TR 62627-03-02-2011	Fiber optic interconnecting devices and passive components - Part 03-02: Reliability - Report of high power transmission test of specified passive optical components 光纤无源器件和无源组件——第 03-02 部分: 可靠性——指定无源光纤组件大功率传输试验的报告
	IEC 62660-2-2010	Secondary lithium-ion cells for the propulsion of electric road vehicles - Part 2: Reliability and abuse testing 电气公路用车的驱动用辅助锂电池——第 2 部分: 可靠性和滥用试验
	IEC/TR 62721-2012	Reliability of devices used in fibre optic systems - General and guidance 光纤系统用器件的可靠性——总则和指南
方法标准	IEC 61164-2004	Reliability growth - Statistical test and estimation methods 可靠度增长——统计试验和估计方法
	IEC 62308-2006	Equipment reliability - Reliability assessment methods 设备可靠性——可靠性评价方法
	IEC 62343-2-2011	Dynamic modules - Part 2: Reliability qualification 动态模块——第 2 部分: 可靠性鉴定
	IEC 61069-5-1994	Industrial-process measurement and control - Evaluation of system properties for the purpose of system assessment - Part 5: Assessment of system dependability 工业处理测量和控制——系统评定用系统特性估计——第 5 部分: 系统可靠性评定
	IEC 61078-2006	Analysis techniques for dependability - Reliability block diagram and boolean methods 可靠性分析技术——可靠性方框图和布尔代数法
	IEC 60605-4-2001	Equipment reliability testing - Part 4: Statistical procedures for exponential distribution - Point estimates, confidence intervals, prediction intervals and tolerance intervals 设备可靠性试验——第 4 部分: 指数分布的统计方法——点估计、置信区间、预测区间和公差区间

(续表)

标准类型	标准编号	标准名称
方法标准	IEC 60605-6-2007	Equipment reliability testing - Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity 设备可靠性试验——第 6 部分：对恒定失效率 and 恒定失效密度有效性和估计的试验
	IEC 60749-30-2011	Semiconductor devices – Mechanical and climatic test methods –Part 30: Preconditioning of non-hermetic surface mount devices prior to reliability testing 半导体器件——机械和气候试验方法——第 30 部分：可靠性试验前不气密的表面安装器件的预调
	IEC 62278-2002	Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) 铁路设施——可靠性、有效性、维修性和安全性 (RAMS) 的规范和论证
管理标准	IEC/TS 62686-1-2012	Process management for avionics - Electronic components for aerospace, defence and high performance (ADHP) applications - Part 1: General requirements for high reliability integrated circuits and discrete semiconductors 航空电子设备过程管理——航空航天、国防和高性能 (ADHP) 应用程序用电子组件——第 1 部分：高可靠性和离散半导体集成电路通用要求

11.2.3 ISO 制定的可靠性标准

ISO 标准是指由国际标准化组织制定的标准。国际标准化组织是一个由国家标准化机构组成的世界范围的联合会。根据该组织章程，每一个国家只能有一个最有代表性的标准化团体作为其成员，原国家质量技术监督局以 CSBTS 名义国参加 ISO 活动。

ISO 的前身是国际标准化协会 (International Standards Association, ISA)，ISA 成立于 1926 年 (1926 年美、英、加等七国标准化机构第三次代表联席会议决定成立国际标准化协会，并于 1928 年成立)。第二次世界大战的爆发，迫使 ISA 停止工作。战争结束后，大环境为工业恢复提供了条件，于是 1946 年 10 月，来自 25 个国家标准化机构的领导人在伦敦聚会，讨论成立国际标准化组织的问题，并把这个新组织称为 ISO。会议一致通过了 ISO 章程和议事规则。1947 年 2 月 23 日 ISO 开始正式运行，ISO 的中央办事机构设在瑞士的日内瓦，中国既是发起国又是首批成员国。

ISO 的组织机构包括：ISO 全体大会、主要官员、成员团体、通信成员、捐助成

员、政策发展委员会、合格评定委员会（CASCO）、消费者政策委员会（COPOLCO）、发展中国家事务委员会（DEVCO）、特别咨询小组、技术管理局、技术委员会 TC、理事会、中央秘书处等。

ISO 的技术活动是制定并出版国际标准（International Standards）。ISO 的工作涉及除电工标准以外的各个技术领域的标准化活动。进入 20 世纪 90 年代以后，通信技术领域的标准化工作展现出快速的发展趋势，成为国际标准化活动的重要组成部分。ISO 与国际电工委员会（IEC）和国际电信联盟（ITU）加强合作，相互协调，三大组织联合形成了全世界范围标准化工作的核心。ISO 与 IEC 共同制定了《ISO/IEC 技术工作导则》，该导则规定了从机构设置到人员任命以及各人职责的一系列细节，把 ISO 的技术工作从国际一级到国家一级再到技术委员会（Technical Committee 简称 TC）、分委员会（Sub-Committee，简称 SC），最后到工作组（Working Group，简称 WG）连成一个有机的整体，从而保证了这个具有成员国、技术委员会、分委员会及工作组和 30000 名专家参加的国际化庞大机构的有效运转。截至目前，ISO 已经发布近 14000 项国际标准、技术报告及相关指南，而且尚在不断增加之中。为制定这些标准，平均每个工作日有 15 个 ISO 会议在世界各地召开。

ISO 的工作引起了各国际组织的兴趣，535 个国际组织与 ISO 的技术委员会和分委员会建立了联络关系。为沟通信息，ISO 建立了情报网（ISONET），已经有 82 个国家的标准信息中心向该网提供快速存取，网络已经收入 500 000 件标准、技术法规和其他标准类出版物，有 10 750 个国际标准和 2700 个国际标准草案的录入数据。ISO 制定的可靠性国际标准如表 11-2 所示。

表 11-2 ISO 制定的可靠性国际标准

标准类型	标准编号	标准名称
基础通用标准	ISO 2394-1998	General principles on reliability for structures 结构可靠性的一般原则
	ISO 6527-1982	Nuclear power plants -- Reliability data exchange -- General guidelines 核电站——可靠性资料交换——一般导则
	ISO 7385-1983	Nuclear power plants -- Guidelines to ensure quality of collected data on reliability 核电站——收集可靠性资料的质量保证导则
	ISO 8107-1993	Nuclear power plants -- Maintainability -- Terminology 核电站——维修性——术语
	ISO 8930-1987	General principles on reliability for structures -- List of equivalent terms 结构可靠性的一般原则——等义术语表（三种语言版）
	ISO 14224-2006	Petroleum, petrochemical and natural gas industries -- Collection and exchange of reliability and maintenance data for equipment 石油和天然气工业——设备可靠性，维护数据的收集和交换

(续表)

标准类型	标准编号	标准名称
基础通用标准	ISO 14461-2-2005	Milk and milk products——Quality control in microbiological laboratories - - Part 2: Determination of the reliability of colony counts of parallel plates and subsequent dilution steps 乳和乳制品——微生物实验室的质量控制——第 2 部分: 平行板和续 馏步骤菌落数可靠性的测定
产品标准	ISO/TR 15801-2009	Document management -- Information stored electronically -- Recommendations for trustworthiness and reliability 文件管理——信息电子化存储—可信赖性和可靠性建议
	ISO 19973-2-2007	Pneumatic fluid power -- Assessment of component reliability by testing -- Part 2: Directional control valves 气压传动——元件可靠性的试验评价——第 2 部分: 方向控制阀
	ISO 19973-3-2007	Pneumatic fluid power -- Assessment of component reliability by testing -- Part 3: Cylinders with piston rod 气压传动——元件可靠性的试验评价——第 3 部分: 带活塞杆的气缸
	ISO 19973-4-2007	Pneumatic fluid power -- Assessment of component reliability by testing -- Part 4: Pressure regulators 气压传动——元件可靠性的试验评价——第 4 部分: 调压器
	ISO 3977-9-1999	Gas turbines —— Procurement -- Part 9: Reliability, availability, maintainability and safety 燃气轮机——采购——第 9 部分: 可靠度、有效性、可维护性及安全
方法标准	ISO 16708-2006	Petroleum and natural gas industries -- Pipeline transportation systems -- Reliability-based limit state methods 石油和天然气工业——管道传输系统——基于可靠性的极限状态法
	ISO/TR 19972-1-2009	Hydraulic fluid power -- Methods to assess the reliability of hydraulic components -- Part 1: General procedures and calculation method 液压传动——液压部件可靠性评估的方法——第 1 部分: 通用程序和 计算方法
	ISO 19973-1-2007	Pneumatic fluid power -- Assessment of component reliability by testing -- Part 1: General procedures 气压传动——元件可靠性的试验评价——第 1 部分: 一般规程
管理标准	ISO 20815-2008	Petroleum, petrochemical and natural gas industries -- Production assurance and reliability management 石油、石化和天然气工业——生产保证和可靠性管理
	ISO 23460-2011	Space projects —— Programme management —— Dependability assurance requirements 航空航天项目——程序管理——可靠保证要求

11.2.4 IEEE 制定的可靠性标准

IEEE 于 1963 年 1 月 1 日由 AIEE（美国电气工程师学会）和 IRE（美国无线电工程师学会）合并而成，是美国规模最大的专业学会。IEEE 是一个非营利性科技学会，拥有全球近 175 个国家 36 万名会员。通过多元化的会员，该组织在太空、计算机、电信、生物医学、电力及消费性电子产品等领域中都具有极高的权威性。

IEEE 制定的可靠性标准按照标准类型也分为三类：基础通用标准、产品标准和方法标准，如表 11-3 所示。

表 11-3 IEEE 制定的可靠性国际标准

标准类型	标准编号	标准名称
基础通用标准	IEEE 1413-2010	Framework for Reliability Prediction of Hardware 硬件可靠性预计框架
	IEEE 1624-2008	Organizational Reliability Capability 组织可靠性能力
	IEEE 352-1987	Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems (ANSI/IEEE) R (1999) 核电站安全系统可靠度分析通用原则指南
产品标准	IEEE 762 INT 1-2010	Standard Definitions for Use in Reporting Electric Generating Unit Reliability, Availability, and Productivity 发电机组可靠性，有效性和生产率报表使用的标准定义
	IEEE 1332-1998	Standard Reliability Program for the Development and Production of Electronic Systems and Equipment 电子系统、设备开发与生产的可靠性程序
	IEEE 577-2012	Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations 核电站安全系统的设计和运行中的可靠性分析要求
	IEEE 933-1999	Guide for the Definition of Reliability Program Plans for Nuclear Power generating Stations 核电站可靠性计划方案的定义
方法标准	IEEE 1633-2008	Recommended Practice on Software Reliability 软件可靠性的推荐实施规程
	IEEE 1082-1997	Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations R (2003) 核电站人工操作可靠度分析专用指南
	IEEE 1240-2000	Guide for the Evaluation of the Reliability of HVDC Converter Stations 高压直流输电（HDVC）换流站可靠性的评估指南

(续表)

标准类型	标准编号	标准名称
方法标准	IEEE 1366-2012	Guide for Electric Power Distribution Reliability Indices 配电可靠性指数指南
	IEEE 1413.1-2002	Guide for Selecting and Using Reliability Predictions Based on IEEE 1413 基于 IEEE 1413 的可靠性预测的选择和使用指南
	IEEE STD 1792-2011	Recommended Practice for Nuclear Power Generating Station (NPGS) Preferred Power Supply (PPS) Reliability 核电站 (NPGS) 优先电源 (PPS) 可靠性用推荐实施规程

此外，在软件可靠性领域，1988 年，IEEE 制定了第一份关于软件可靠性度量体系方面的标准以及该标准的实施指南。2005 年，IEEE 对软件可靠性度量体系标准进行了修订。2008 年，IEEE 对 R-013-1992 标准进行修订，R-013-1992 标准是 AIAA（美国航空与航天学会）在 1992 年制定的关于软件可靠性评估的标准，这也说明 IEEE 在软件可靠性方面的成绩是国际公认的，IEEE 主要制定了软件可靠性度量体系和评估两方面的标准，分别如表 11-4 和表 11-5 所示。

表 11-4 软件可靠性度量体系标准

标准类型	标准编号	标准名称
应用标准	IEEE Std 982.2-1988	软件可靠性度量实施指南
工具标准	IEEE Std 982.1-2005	软件可信性度量词典

表 11-5 软件可靠性评估标准

标准类型	标准编号	标准名称
应用标准	AIAA/ANSI R-013-1992	软件可靠性操作规程
应用标准	IEEE Std 1633-2008	软件可靠性操作规程

11.3

可靠性国家标准/国家军用标准

11.3.1 可靠性国家标准

国家标准分为强制性国标（GB）和推荐性国标（GB/T）。国家标准的编号由国家标准的代号、国家标准发布的顺序号和国家标准发布的年号（发布年份）构成。强制性国标是保障人体健康、人身、财产安全的标准和法律，以及行政法规规定强制执行的国家标准；推荐性国标是指生产、检验、使用等方面，通过经济手段或市

场调节而自愿采用的国家标准。但推荐性国标一经接受并采用，或各方商定同意纳入经济合同中，就成为各方必须共同遵守的技术依据，具有法律上的约束性。现行主要的可靠性国家标准如表 11-6 所示。

表 11-6 主要的可靠性国家标准

标准类型	标准编号	标准名称
基础通用标准	GB/T 2900.13-2008	电工术语可信性与服务质量
	GB/T 6992.2-1997	可信性管理第 2 部分：可信性大纲要素和工作项目
	GB/T 5080.1-1986	设备可靠性试验总要求
	GB/T 5080.2-1986	设备可靠性试验的试验周期设计导则
	GB/T 5080.4-1985	在设备可靠性试验中可靠性测定试验的点估计和区间估计方法（指数分布）
	GB/T 5080.5-1985	设备可靠性试验成功率的验证试验方案
	GB/T 5080.6-1996	设备可靠性试验恒定失效率假设的有效性检验
	GB/T 5080.7-1986	设备可靠性试验在恒定失效率假设下的失效率与平均无故障时间的验证试验方案
	GB/T 5081-1985	电子产品现场工作可靠性、有效性和维修性数据的收集指南
	GB/T 7288.1-1987	设备可靠性试验推荐的试验条件用室内便携设备粗模拟
	GB/T 7288.2-1987	设备可靠性试验推荐的试验条件固定使用在有气候防护场所设备精模拟
	GB/T 7289-1987	可靠性、维修性与有效性预计报告编写指南
	GB/T 7826-1987	系统可靠性分析技术失效模式和效应分析（FMEA）程序
	GB/T 7827-1987	可靠性预计程序
	GB/T 7828-1987	可靠性设计评审
	GB/T 7829-1987	故障树分析程序
	GB/T 9414.1-1988	设备维修性导则第一部分：维修性导言（整修 A）
	GB/T 9414.3-1988	设备维修性导则第三部分：维修性大纲（整修 A）
	GB/T 9414.2-1988	设备维修性导则第二部分：规范与合同中的维修性要求
	GB/T 9414.4-1988	设备维修性导则第五部分：设计阶段的维修性研究
	GB/T 9414.5-1988	设备维修性导则第六部分：维修性检验（整修 B）
	GB/T 9414.6-1988	设备维修性导则第七部分：维修性数据的收集、分析与表示（整修 B）
	GB/T 9414.7-2000	设备维修性导则第四部分：诊断测试
	GB/T 9414.8-2001	设备维修性导则第九部分：维修性评价的统计方法
	GB/T 15174-1994	可靠性增长大纲
	GB/T 15647-1995	稳态可用性验证试验方法

(续表)

标准类型	标准编号	标准名称
基础通用标准	GB/T 18272.5-2000	工业过程测量和控制系统评估中系统特性的评定第 5 部分：系统可信性评估
	GB/T 5271.14-2008	信息技术词汇第 14 部分：可靠性、可维护性与可用性
	GB/T 23567.1-2009	数控机床可靠性评定第 1 部分：总则
	GB/T 23568.1-2009	机床功能部件可靠性评定第 1 部分：总则
	GB/T 7163-2008	核电厂安全系统的可靠性分析要求
	GB/T 9225-1999	核电厂安全系统可靠性分析一般原则
	GB/T 15510-2008	控制用电磁继电器可靠性试验通则
	GB/Z 10962-2008	机床电器可靠性通则
	GB 50144-2008	工业建筑可靠性鉴定标准
	GB 50153-2008	工程结构可靠性设计统一标准
	GB 50292-1999	民用建筑可靠性鉴定标准
产品标准	GB/T 15279-2002	自动电话机技术条件
	GB/T 18185-2000	水文仪器可靠性技术要求
	GB/T 20172-2006	石油天然气工业设备可靠性和维修数据的采集与交换
	GB/T 21194-2007	通信设备用的光电子器件的可靠性通用要求
	GB/T 24108-2009	岩土工程仪器可靠性技术要求
	GB/T 24262-2009	石油物探仪器环境试验及可靠性要求
	GB/T 24468-2009	半导体设备可靠性、可用性、维修性（RAM）的定义和测量规范
方法标准	GB/T 9382-1988	彩色电视广播接收机可靠性验证试验贝叶斯方法
	GB/T 5374-2008	摩托车和轻便摩托车可靠性试验方法
	GB/T 11463-1989	电子测量仪器可靠性试验
	GB/T 12165-1998	盒式磁带录音机可靠性要求和试验方法
	GB/T 12322-1990	通用型应用电视设备可靠性试验方法
	GB/T 12678-1990	汽车可靠性行驶试验方法
	GB/T 12840-1996	盒式磁带录音机运带机构可靠性要求和试验方法
	GB/T 13426-1992	数字通信设备的可靠性要求和试验方法
	GB/T 14127-1993	黑白电视接收机可靠性验证试验贝叶斯方法
	GB/T 15214-2008	超声诊断设备可靠性试验要求和方法
	GB/T 15524-1995	非广播磁带录像机可靠性要求和试验方法
	GB/T 15844.3-1995	移动通信调频无线电话机可靠性要求及试验方法
	GB/T 19055-2003	汽车发动机可靠性试验方法
	GB/T 21975-2008	起重及冶金用三相异步电动机可靠性试验方法
	GB/T 22758-2008	家用电动洗衣机可靠性试验方法

(续表)

标准类型	标准编号	标准名称
方法标准	GB/T 22759-2008	家用和类似用途的制冷器具可靠性试验方法
	GB/T 24607-2009	滚动轴承寿命与可靠性试验及评定
	GB/T 24985-2010	家用和类似用途房间空气调节器可靠性试验方法
	GB/T 24986.1-2010	家用和类似用途电器可靠性评价方法第 1 部分：通用要求
	GB/T 24986.2-2010	家用和类似用途电器可靠性评价方法第 2 部分：电冰箱（电冰柜）的特殊要求
	GB/T 24986.3-2010	家用和类似用途电器可靠性评价方法第 3 部分：洗衣机的特殊要求
	GB/Z 22074-2008	塑料外壳式断路器可靠性试验方法
	GB/Z 22200-2008	小容量交流接触器可靠性试验方法
	GB/Z 22201-2008	接触器式继电器可靠性试验方法
	GB/Z 22202-2008	家用和类似用途的剩余电流动作断路器可靠性试验方法
	GB/Z 22203-2008	家用及类似场所用过电流保护断路器的可靠性试验方法
	GB/Z 22204-2008	过载继电器可靠性试验方法
管理标准	GB/T 14394-2008	计算机软件可靠性和可维护性管理

11.3.2 可靠性国家军用标准

标准化是用标准统一思想、建立流程、规范行为的过程，标准的确立与普及也必然会对文化产生促进和推动作用。加强军用标准化建设是实现强军目标的重要技术支撑，发展先进军事文化是实现强军目标的重要思想政治保障。在强军目标的统领下，军用标准化建设与先进军事文化建设应该在人的素质塑造上共同发力，确保军魂、军力、军风在打赢明天战争的目标下实现有机融合。要通过军用标准化工作，用标准的统一协调，深化全军官兵面向未来信息化作战的一体化思想；用标准的规范精神，雕刻当代军人严谨务实、规范精细、注重品质、刻苦钻研的优良作风；用标准的先进理念，烘焙全军通过技术创新、管理创新谋求战斗力生成模式转变的浓郁氛围。

由于国际标准和国外先进标准代表了先进技术的发展方向，是先进技术和成功经验的结晶和总结。积极采用国际标准和国外先进标准，一方面可以使我们的标准化工作和国际接轨，另一方面可以促进我们的标准水平的提高，所以采用国际标准和国外先进标准是我国的一项重要重要的技术经济政策，是技术引进的重要组成部分。它对促进技术进步，提高产品质量，发展社会主义市场经济，适应国际贸易，具有

重要的作用。积极采用国外先进军用标准可以强化武器装备研制过程的管理,提高武器装备的质量,缩短研制周期,降低研制成本。对提高我国的国防实力具有非常积极的促进作用。

我国的军用标准化工作起步于 20 世纪 80 年代初。30 年来,军用标准化工作经历从有到无,由弱到强,从分散管理到集中统一管理的过程,军用标准体系基本建成,标准贯彻实施逐步加强,武器装备的通用化、系列化、组合化取得丰硕成果,全军标准化意识明显提高,人才队伍不断壮大,基础建设稳步推进,军用标准化综合效益得到较好发挥,为国防和军队现代化建设做出了重要贡献。

军用标准化工作面向军事斗争准备、面向军队信息化建设、面向重大工程和重点武器装备建设、面向提高部队战斗力,坚持“有所为,有所不为”,大力加强战略谋划,积极推进军民融合,基本建成覆盖作战指挥、军事训练、政治工作、后勤保障、武器装备和国防科技工业等国防和军队现代化建设主要领域,水平先进、科学实用的军用标准体系。目前,国家军用标准总数量达到 12 000 多项,在国防和军队现代化建设中,充分发挥了引领规范、支撑服务和监督保障作用。

国军标是为了保证军用元器件的质量,对元器件所制定的一系列的标准与要求,以备对航天等部门提供优质的元器件。为了保证军用元器件的质量,我国制定了一系列的元器件标准。在 20 世纪 70 年代末期制定的“七专”7905 技术协议和 20 世纪 80 年代初期制定的“七专”8406 技术条件(以下统称“七专”条件)，“七专”技术条件是建立我国军用元器件标准的基础,目前按“七专”条件或其加严条件控制生产的元器件仍是航天等部门使用的主要品种(注:“七专”是指专人、专机、专料、专批、专检、专技、专卡或专线)。

最早的的质量认证是七专线审查,由当时的五所(现在的工信部电子五所)数据中心审查,依据规定,必须经“七专线”及产品经过审核、批准、公布(七专目录)的产品,才可以打上“G”的标记。

自 20 世纪 90 年代初期开始的军标认证,是依据国家军用标准的认证。其认证机构是由原国防科工委授权的中国军用电子元器件质量认证委员会,它独立于元器件的生产方和使用方,所以属于第三方认证。

质量认证包括两方面的内容:对于元器件生产单位质量保证能力的评定;对其所生产的元器件进行鉴定或考核,合格者列入合格产品目录(QPL)或合格生产厂目录(QML)。

除了原国防科工委授权的军用电子元器件质量认证机构外,军工行业也可授权具有认证能力的单位按标准或法规性文件,对元器件生产单位的质量保证能力进行考察,以及对其生产的产品进行鉴定或考核,合格者列入该军工行业合格产品目录。为了区别于由国家授权的质量认证,将军工行业授权的质量认证,称为质量认定,由于军工行业是元器件的用户,所以质量认定也可称为用户认证或第二方认证。

凡已通过质量认证，其认证条件能满足军工产品质量要求的元器件，可不再进行质量认定。凡未经过质量认证或其认证条件不能满足军工产品质量要求的元器件及其生产单位，军工行业的有关部门认为必要时可组织人员进行质量认定。可靠性国军标是保证我国成功研制、生产出可靠的器件，以及对这些器件进行有效的检验、使用和维护的重要依据。

在系统可靠性标准方面，我国制定了 GJB 450A、GJB 899A 和 GJB/Z 299C 等涉及可靠性管理、论证、分析、设计、试验和使用阶段数据收集和评估等方面的技术标准。

目前，我国军用可靠性标准形成体系化，覆盖基础通用、产品、方法和管理等类别。现行的主要可靠性国家军用标准如表 11-7 所示。

表 11-7 主要的可靠性国家军用标准

标准类型	标准编号	标准名称
基础通用标准	GJB 450A-2004	装备可靠性工作通用要求
	GJB 451A-2005	可靠性维修性保障性术语
	GJB 546-1988	电子元器件可靠性保证大纲
	GJB 630A-1998	飞机质量与可靠性信息分类和编码要求
	GJB 899A-2009	可靠性鉴定和验收试验
	GJB 1407-1992	可靠性增长试验
	GJB 1686-1993	装备质量与可靠性信息管理要求
	GJB 1775-1993	装备质量与可靠性信息分类和编码通用要求
	GJB 1909A-2009	装备可靠性、维修性、保障性要求论证
	GJB 3334-1998	舰船质量与可靠性信息分类和编码要求
	GJB 3386-1998	航天系统质量与可靠性信息分类和编码要求
	GJB 3469-1998	导弹武器系统质量与可靠性信息分类和编码要求
	GJB 3554-1999	车辆系统质量与可靠性信息分类和编码要求
	GJB 3555-1999	火炮系统质量与可靠性信息分类和编码要求
	GJB/Z 23-1991	可靠性和维修性工程报告编写一般要求
	GJB/Z 27-1992	电子设备可靠性热设计手册
	GJB/Z 72-1995	可靠性、维修性评审指南
	GJB/Z 102-1997	软件可靠性和安全性设计准则
	GJB/Z 108A-2006	电子设备非工作状态可靠性预计手册
	GJB/Z 299C-2006	电子设备可靠性预计手册
产品标准	GJB 62-1985	有可靠性指标的精密聚苯乙烯电容器总规范
	GBJ 144-1990	工业厂房可靠性鉴定标准
	GJB 62/1-1985	CB14K 型有可靠性指标的非密封精密聚苯乙烯电容器详细规范

(续表)

标准类型	标准编号	标准名称
产品标准	GJB 63B-2001	有可靠性指标的固体电解质钽电容器总规范
	GJB 65B-1999	有可靠性指标的电磁继电器总规范
	GJB 67.6-1985	军用飞机强度和刚度规范可靠性要求和疲劳载荷
	GJB 86.5-1986	机载火控雷达战术性能定型试验规程在试验阶段的可靠性特征值统计
	GJB 191A-1997	有可靠性指标的云母固定电容器总规范
	GJB 192A-1998	有可靠性指标的无封装多层片式瓷介电容器总规范
	GJB 244-1987	有可靠性指标的薄膜固定电阻器总规范
	GJB 244/1-1987	RJK52 型有可靠性指标的金属膜固定电阻器详细规范
	GJB 244/2-1987	RJK53 型有可靠性指标的金属膜固定电阻器详细规范
	GJB 244/3-1987	RJK54 型有可靠性指标的金属膜固定电阻器详细规范
	GJB 244/4-1987	RJK55 型有可靠性指标的金属膜固定电阻器详细规范
	GJB 244/5-1987	RJK56 型有可靠性指标的金属膜固定电阻器详细规范
	GJB 468-1988	有可靠性指标的和没有可靠性指标的 1 类瓷介电容器总规范
	GJB 473.8-1988	舟桥器材设计定型试验规程可靠性试验
	GJB 540.7-1991	飞航导弹强度和刚度规范可靠性要求和重复载荷
	GJB 403.5-1987	舰载雷达通用技术条件可靠性要求
	GJB 701.10-1989	地面雷达情报处理和传递系统通用技术条件系统可靠性考核方法
	GJB 837.3-1990	布雷火箭弹定型试验规程点火系统可靠性试验
	GJB 796.8-1990	军用固定桥深器材设计定型试验规程可靠性试验
	GJB 806.6-1990	陆地战略导弹通用规范可靠性要求
	GJB 1130-1991	飞机弹射救生系统可靠性和维修性通用要求
	GJB 1909.3-1994	装备可靠性、维修性参数选择和指标确定要求核战斗部
	GJB 1909.4-1994	装备可靠性、维修性参数选择和指标确定要求卫星
	GJB 1909.5-1994	装备可靠性、维修性参数选择和指标确定要求军用飞机
	GJB 1909.6-1994	装备可靠性、维修性参数选择和指标确定要求舰船
	GJB 1909.7-1994	装备可靠性、维修性参数选择和指标确定要求装甲车辆和军用汽车
	GJB 1909.9-1994	装备可靠性、维修性参数选择和指标确定要求弹药
	GJB 1909.10-1998	装备可靠性、维修性参数选择和指标确定要求电子系统
	GJB 2225.3-1994	地面电子对抗设备通用技术要求可靠性要求
	GJB 2226.9-1994	舰载雷达情报系统通用要求可靠性、维修性要求
	GJB 2515-1995	弹药储存可靠性要求
	GJB 1909.8-1994	装备可靠性、维修性参数选择和指标确定要求火炮
	GJB 3655-1999	火炮储存可靠性要求
	GJB 4005-2000	地雷爆破器材可靠性要求

(续表)

标准类型	标准编号	标准名称
方法标准	GJB 74.7-1985	军用地面雷达通用技术条件可靠性试验方法
	GJB 81.18-1985	军用推土机设计定型试验规程可靠性试验方法
	GJB 16-1984	地面炮瞄雷达可靠性试验方法
	GJB 349.33-1990	常规兵器定型试验方法反坦克导弹系统可靠性试验
	GJB 367.3-1987	军用通信设备通用技术条件可靠性鉴定试验和验收试验方法
	GJB 376-1987	火工品可靠性评估方法
	GJB 403.6-1987	舰载雷达通用技术条件可靠性试验方法
	GJB 522.5-1988	气象情报接收设备技术条件可靠性试验方法
	GJB 570.6-1988	气象仪器定型试验方法可靠性试验
	GJB 573.18-1988	引信环境与性能试验方法顺序振动—装卸可靠性试验
	GJB 838.3-1990	反坦克侧甲雷定型试验规程命中可靠性试验方法
	GJB 838.5-1990	反坦克侧甲雷定型试验规程触发引信发火可靠性试验方法
	GJB 839.4-1990	反坦克车底地雷定型试验规程传爆可靠性试验方法
	GJB 840.4-1990	反坦克履带地雷定型试验规程传爆可靠性试验方法
	GJB 840.12-1990	反坦克履带地雷定型试验规程引信发火可靠性试验方法
	GJB 1621.8A-2006	技术侦察装备通用技术要求第 8 部分：可靠性指标和验证试验方法
	GJB 968.11-1990	军用舷外机定型试验规程可靠性试验方法
	GJB 1009.9-1990	防步兵跳雷定型试验规程发火可靠性试验方法
	GJB 3196.50A-2005	枪弹试验方法第 50 部分：枪弹对枪械机构动作可靠性试验
	GJB 3637-1999	地面压制火炮可靠性、维修性要求与验证
	GJB 3651-1999	小口径高炮可靠性维、修性要求与验证
	GJB 3676-1999	军用工程机械可靠性、维修性要求
	GJB 3752.9-1999	地地战略导弹武器系统作战使用要求论证方法可靠性和维修性
	GJB 4110.17-2000	军用轮式工程机械设计定型通用试验规程可靠性试验方法
	GJB 4111.25-2000	军用履带式工程机械设计定型通用试验规程可靠性试验方法
	GJB 4622-1993	四折带式舟桥设计定型试验规程可靠性试验
	GJB 5489.13-2005	航空机枪试验方法第 13 部分：可靠性
	GJB 5495.9-2005	榴弹发射器试验方法第 9 部分：可靠性试验
	GJB 5496.20-2005	航空炸弹试验方法第 20 部分：安全性、可靠性试验挂飞投放安全性
	GJB 5496.21-2005	航空炸弹试验方法第 21 部分：安全性、可靠性试验开伞可靠性
	GJB 5496.22-2005	航空炸弹试验方法第 22 部分：安全性、可靠性试验航空子母炸弹开箱可靠性
	GJB 6399-2008	导弹和运载火箭用液压泵可靠性要求和试验方法
	GJB 6458.30-2008	火箭炮试验方法第 30 部分：可靠性试验
	GJB 6462-2008	航炮可靠性鉴定和验收试验

(续表)

标准类型	标准编号	标准名称
方法标准	GJB 6478-2008	火工品可靠性计量——计数综合评估方法
	GJB 6556.5-2008	军用气象装备定型试验方法第5部分：可靠性和维修性
	GJB 736.10-1990	火工品试验方法电火工品金属桥丝焊接可靠性试验
管理标准	GJB/Z 77-1995	可靠性增长管理手册
	GJB 3872-1999	装备综合保障通用要求
	GJB-Z 4-1988	质量成本管理指南
	GJB 2993-1997	武器装备研制项目管理
	GJB 1406A-2005	产品质量保证大纲
	GJB546A-1996	电子元器件质量保证大纲
	GJB/Z106A-2005	工艺标准化大纲编制指南
	GJB/Z114A-2005	产品标准化大纲编制指南
	GJB 5852-2006	装备研制风险分析要求
	GJB 2102-1994	合同中质量保证要求
	GJB 6388-2008	装备综合保障计划编制要求
	GJB/Z147-2006	装备综合保障评审指南
	GJB 439-1998	军用软件质量保证规范
	GJB 5234-2004	军用软件验证和确认
	GJB 1268A-2004	军用软件验收要求
	GJB 3206A-2010	技术状态管理
	GJB 571A-2005	不合格品管理
	GJB 5423-2005	质量管理体系的财务资源
	GJB/Z127A-2006	装备质量管理统计方法应用指南
	GJB 841-1990	故障报告、分析和纠正措施系统
	GJB/Z1391A-2006	故障模式、影响及危害性分析指南
	GJB 466-1998	理化试验质量控制要求
	GJB 1442A-2006	检验工作要求
	GJB 5109-2004	装备计量保障通用要求监测和校准

11.4 美国军用可靠性标准

美国军用标准的内容十分丰富，它包括了通用技术标准，以及武器、弹药、飞机、舰艇、车辆、电子设备、仪器仪表、元器件、材料、数据处理设备、发动机、机械、空调、消防救生、水暖、净水设备，乃至药品、办公用品、文体用品、服

装、食品、化妆品等 76 个大类，约 570 个小类（另有 30 个文字类）。美国军用标准是在美国国防部直接领导下制定的。制定军用标准的目的在于，保证在整个国防系统中实现产品和服务的标准化、系列化、通用化。现行的国防部命令 DOD 4120.3《国防部标准化和规范大纲》是全军标准化工作的准绳。该大纲中所有的规范、标准、手册、图纸以及有关标准文件组成了一个国防标准化文件体系。

美军标准与规范依其特性大体分为 3 类，即：军用标准（MIL-STD-xxxxx）一般是说明需求和“这是什么”的文件；军用手册（MIL-HDBK-xxxxx）一般则是“为什么”的文件；军用规范（MIL-X-00000）则大多是以特定的军品为对象的详细产品规范，其中 X 为代表规范名称的第一个字母；还有一些单独的美军规范以 MS 00000 为编号，是美军规范的扩充与延伸，美军可靠性标准亦满足这一规律。

美国军用标准多年来一直扮演着研究开发可靠性相关标准文件的带头角色，也是最早制定可靠性标准的。从 20 世纪 50 年代后期开始颁发有关可靠性标准，例如：美国国防部 1957 年 1 月发布了 MIL-R-25717《电子设备可靠性保证大纲》，1958 年 6 月发布了 MIL-STD-441《军用电子设备的可靠性》，1959 年 1 月发布了 IL-R-27542《宇航系统、分系统及设备的可靠性大纲要求》等。20 世纪 60 年代美国的可靠性工程进入了全面的发展阶段，这个阶段也是美军可靠性标准大量发布的时期。MILSTD-785《系统与设备的可靠性大纲要求》、MILSTD-781《可靠性试验、指数分布》、MIL-HDBK-217《电子设备可靠性预计》等许多重要标准，都是在这个时期先后发布的。20 世纪 70 年代后，随着美国可靠性工程的深入发展，这些标准得到了进一步的修改和完善，并又颁发了许多新的标准。20 世纪 80 年代末，美国军方从最新的全面质量管理的原理出发，研究并推行产品保证的管理。从 20 世纪 90 年代开始，美军启动了对军用可靠性标准和规范的变革工作，并提出最大限度地减少对军用标准和规范的依赖，更多地采用民用标准和规范，以达到充分利用民用先进技术的目的。由此，MIL-Q-9858A《质量大纲要求》于 1994 年被废止，由民用标准 ISO 9000-ANSI/ASQC Q90 系列取代；MIL-HDBK-217《电子设备的可靠性预计》在 1995 年被废止，由民用标准 Tlecordia SR-32《电子设备的可靠性预计》取代；MIL-STD-785B《设备、系统研制和生产阶段的可靠性大纲》于 1998 年被废止，由民用标准 IEEE I332《电子系统、设备的研制和生产可靠性大纲》取代。

美国军用标准并没有为此规划专门的标准体系，而是按照专业分类制定了一系列标准。大致可分为：可靠性名词定义、需求标准与规范、可靠性管理标准与规范、可靠性工程标准与规范、可靠性试验标准与规范等几大类。美军标的可靠性标准与产品保证各个领域中的标准互相支持，形成了相应的标准体系，美国军用可靠性标准体系的结构示意图如图 11-2 所示。

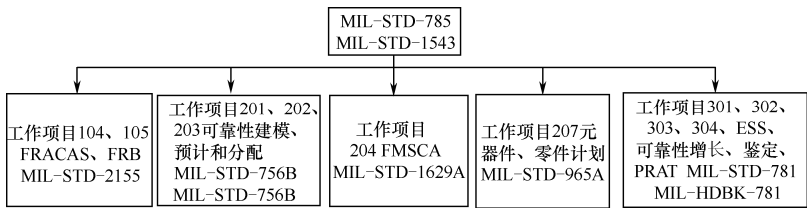


图 11-2 美国军用可靠性标准体系的结构示意图

现行的美国主要可靠性军用标准如表 11-8 所示。

表 11-8 美国主要可靠性军用标准

标准类型	标准编号	标准名称
基础通用标准	MIL-STD-721C	可靠性维修性术语
	MIL-HDBD-59A	计算机辅助采办与综合保障实施指南
	MIL-HDBD-217F-1995	电子设备可靠性预计手册
	MIL-HDBD-251-1978	电子产品可靠性热设计手册
	MIL-HDBD-263B-1995	保护电气和电子部件、组件和设备（不包括电气触发爆炸装置）静电放电控制手册
	MIL-HDBD-338B-1998	电子设备可靠性设计手册
	MIL-HDBD-344A-1993	电子产品环境应力筛选指南
	MIL-HDBD-470-1997	装备维修性预计与分配手册
	MIL-HDBD-765	军用电气系统安全设计手册
	MIL-HDBD-2165A-1993	系统和设备可测试性大纲
	MIL-STD-415D	测试性设计准则
	MIL-STD-790F-1995	有可靠性指标和高可靠电工、电子和光纤元器件规范 QPL 体系
	MIL-STD-882C-1998	系统安全性通用大纲
	MIL-STD-1304	可靠性和维修性工程报告编写一般要求
	MIL-STD-1309D-1992	测试性与诊断术语
	MIL-STD-1379D	装备训练规划要求
	MIL-STD-1388/1A	装备保障性分析
	MIL-STD-1388/1B	装备保障性分析记录
	MIL-HDBD-764	系统安全工程手册
方法标准	MIL-HDBD-108	寿命试验抽样程序和表
	MIL-HDBD-781A-1996	可靠性鉴定和验收试验
	MIL-HDBD-2164A-1996	电子设备环境应力筛选过程
	MIL-STD-690C-1993	失效率抽样方案和程序
	MIL-STD-1635	可靠性增长试验



(续表)

标准类型	标准编号	标准名称
方法标准	MIL-STD-1843	装备预防性维修大纲的制定要求与方法
	MIL-STD-2074	可靠性试验故障分类
	MIL-STD-2068	可靠性研制试验
	MIL-STD-2164	电子产品环境应力筛选
	MIL-STD-2111-1986	电子设备的整修、翻修和修理
管理规范	MIL-HDBD-189-1981	可靠性增长管理手册
	MIL-STD-965	电子元器件选用管理要求
	MIL-STD-2155	故障报告、分析和纠正措施系统
	MIL-STD-8866C-1994	飞机强度和刚度的可靠性要求（反复加载、疲劳和损伤容限）
	MIL-STD-24534A-1991	计划维修体系：维修卡要求、维修目录页及有关文件的编制

11.5 可靠性行业标准

11.5.1 核电可靠性标准

核电可靠性是在规定的寿命周期内，在保护人和环境不受超过限度的电离辐射和放射性损害的条件下，持续正常实现相应功能的能力，为了保证核电系统的可靠性，不仅要从设计入手，而且要在制造和管理上采取严格的可靠性规范，按照相应的标准流程进行操作，在系统设计、制造、调试、运行的各个阶段进行对应的可靠性试验，开展相应的评估。为了保证这一过程的顺利开展和实施，国内外相关组织和部门根据系统特点和实际情况，制定了相应的可靠性规范。除了以上可靠性国际标准、国标、国军标中给出的可靠性标准以外，我国核电主要的可靠性标准如表 11-9 所示。

表 11-9 核电主要的可靠性标准

标准类型	标准编号	标准名称
基础通用标准	EJ/T 888-1994	核电厂电气、电子和敏感元件可靠性数据的收集和提供导则
	EJ/T 1165-2002	核工业产品质量、可靠性信息分类与编码要求
	EJ/T 436-1989	核仪器可靠性试验
	NB/T 20183-2012	核电厂可靠性保证大纲编写指南

11.5.2 电力可靠性标准

电力可靠性是电网及设备在规定的时间内按照规定的质量标准不间断输送、供

应电力或实现规定功能要求的能力，对电力系统实施规范化管理是对电力系统和设备的全面质量管理和全过程的安全管理，适合现代化电力行业发展的特点，是实现电力工业现代化的一个重要方面，是对供电系统的规划、设计、基建、施工、设备选型、生产运行和供电服务等方面质量和水平的综合体现。

为了实现对电力系统的规范化管理，相关部门和单位制定了相应的规范和标准，对电力系统从构成系统的最小单元设备到整个系统的实施操作、管理进行规范化、流程化说明。除了以上可靠性国际标准、国标、国军标中给出的可靠性标准以外，电力主要的可靠性标准如表 11-10 所示。

表 11-10 电力主要的可靠性标准

标准类型	标准编号	标准名称
基础通用标准	DL/T 261-2012	火力发电厂热工自动化系统可靠性评估技术导则
	DL/T 302.1-2011	火力发电厂设备维修分析技术导则第 1 部分：可靠性维修分析
	DL/T 861-2004	电力可靠性基本名词术语
	DL/T 1033.11-2006	电力行业词汇第 11 部分：事故、保护、安全和可靠性
产品标准	DL/T 793-2012	发电设备可靠性评价规程
	DL/T 836-2012	供电系统用户供电可靠性评价规程
	DL/T 837-2012	输变电设施可靠性评价规程
	DL/T 989-2005	直流输电系统可靠性评价规程
	DL/T 1090-2008	串联补偿系统可靠性统计评价规程

11.5.3 汽车可靠性标准

汽车的使用环境比一般的消费电子要严酷很多，包括了温度、湿度、振动、雨水、耐老化性能、电压波动以及电压冲击等因素，表 11-11、表 11-12 和表 11-13 给出了不同部位的汽车电子的温度、湿度和振动条件。汽车电子的可靠性要求也比普通消费电子的可靠性要求高很多，一般会高出一个甚至两三个数量级。

表 11-11 汽车电子温度环境条件

部位	最大温度
前仪表盘上部	120℃
前仪表盘底部	71℃
客舱地板	105℃
后架	117℃
头枕	83℃

表 11-12 汽车电子湿度环境条件

部位	最大湿度
引擎舱（引擎附近）	38℃，95%
引擎舱（轮片）	66℃，80%
座椅	66℃，80%
侧门周围	38℃，95%
仪表板前部	38℃，95%
地板	66℃，80%
后架	38℃，95%
行李箱	38℃，95%

表 11-13 汽车电子振动环境条件

振动源	频率（Hz）	振动源	频率（Hz）
发动机转矩波动	2~10	发动机转矩波动	50~80
离合器不正	2~10	传动轴夹角	50~80
传动轴夹角	10~20	发动机旋转惯性	100~200
发动机转矩波动	20~50	齿轮的啮合力	400~2000
旋转失衡	20~50		

针对这些问题，国际上一些标准化组织和主流汽车研发企业先后制定了相应的标准，主要有：AEC 系列标准（Automotive electronics council）、ISO 16750 系列标准（主要采用 IEC 标准）、SAE 相关标准、其他相关标准（MIL-STD-202，MIL-STD-750，MIL-5TD-883，EIA-364）、主流车厂试验标准（Volkswagen，General Motors，Mazda，Ford）。

20 世纪 90 年代，克莱斯勒、福特和通用汽车为建立一套通用的零件资质及质量系统标准而设立了汽车电子委员会（AEC），AEC 建立了质量控制的标准。AEC-Q-100 芯片应力测试的认证规范是 AEC 的第一个标准。AEC-Q-100 于 1994 年首次发表，由于符合 AEC 规范的零部件均可被上述三家车厂同时采用，促进了零部件制造商交换其产品特性数据的意愿，并推动了汽车零件通用性的实施，使得 AEC 标准逐渐成为汽车电子零部件的通用测试规范。经过十多年的发展，AEC-Q-100 已经成为汽车电子系统的通用标准。在 AEC-Q-100 之后又陆续制定了针对离散组件的 AEC-Q-101 和针对被动组件的 AEC-Q-200 等规范，以及 AEC-Q001/Q002/Q003/Q004 等指导性原则。

ISO 16750 系列标准是国际标准化组织 ISO 最近几年推出的针对汽车电子的环境可靠性标准，该标准是欧系车常用的标准，并且逐渐被世界各国转化为国家标准，也

逐渐被各企业标准所引用，成为应用比较广泛的汽车电子的环境可靠性标准。该系列标准包括 5 个部分：（1）ISO 16750-1 总则；（2）ISO 16750-2 电气负载；（3）ISO 16750-3 机械负载；（4）ISO 16750-4 气候负载；（5）ISO 16750-5 化学负载，各试验项目则主要采用了国际电工协会（IEC）的相关环境试验标准。

美国汽车工程师协会（SAE）很早就制定了汽车电子的环境可靠性标准，包括至今仍在广泛使用的 SAE J1211 汽车电气部件环境试验标准。SAE J1455 汽车电气部件环境试验标准以及针对电动汽车电池的环境可靠性标准，SAEJ2464 电动汽车电池滥用试验和 SAE J2380 电动汽车电池的振动试验等一系列标准。

除了上述广泛使用的汽车电子的环境可靠性标准外，还有一些针对电子电器部件的可靠性标准也经常被汽车电子行业采用，这些标准包括：

- MIL-STD-202 电子零部件
- MIL-STD-750 半导体部件
- MIL-STD-883 微电路器件
- EIA-364 系列

一些主流车场的试验标准如表 11-14 所示。

表 11-14 主流车场的试验标准

汽车厂家	相关标准
大众	VW 80101 电气电子安装部件检测条件，VW TL 226 汽车内饰喷涂件技术要求
通用	GMW 3172 电气电子零部件环境可靠性分析设计以及验证程序要求，GMN 10083 塑料喷涂件内饰可靠性
马自达	MES PW67600 电子器件技术要求
福特	FLTM BI 系列标准

国内除了以上可靠性国标、国军标中给出的可靠性标准以外，汽车主要的可靠性标准如表 11-15 所示。

表 11-15 汽车主要的可靠性标准

标准类型	标准编号	标准名称
产品标准	JB/T 4030.1-2000	汽车起重机和轮胎起重机试验规范作业可靠性试验
	JB/T 4030.2-2000	汽车起重机和轮胎起重机试验规范行驶可靠性试验
方法标准	QC/T 702-2004	摩托车和轻便摩托车用催化转化器可靠性试验方法

11.5.4 航天可靠性标准

航天领域任何的疏忽或错误都可能对航天任务和航天人员的人身安全构成威

胁，造成严重的后果，引起重大损失。为了规范化航天领域相关工作人员的工作过程，提高航天工作人员的标准化意识，加强标准化管理，在航天产品的设计、研制、生产、使用和维护过程中充分运用标准化的基本原理和方法，提高和保障航天产品的质量，国内以航天标准化研究所为代表的单位开展航天标准的制定，目前除了以上可靠性国际标准、国军标中给出的可靠性标准以外，现行航天主要的可靠性标准如表 11-16 所示。

表 11-16 航天主要的可靠性标准

标准类型	标准编号	标准名称
基础通用标准	QJ 2668-1994	航天产品可靠性设计准则电子产品可靠性设计准则
	QJ 2731A-2011	航天产品质量与可靠性信息分类与代码
	QJ 2874-1997	质量与可靠性信息库命名方法与代码
	QJ 3262-2005	高可靠性实时嵌入式软件设计指南
产品标准	QJ 1408A-1998	航天产品可靠性保证要求
	QJ 1556B-2008	元器件质量与可靠性信息采集卡填写规定
	QJ 2005-1990	控制系统可靠性设计准则
	QJ 2406A-2005	固体火箭发动机可靠性设计要求和评审
	QJ 2933-1997	地（舰）空导弹武器系统可靠性设计与分析指南
	QJ 3153-2002	导弹储存可靠性设计技术指南
	QJ 3231-2005	固体火箭发动机可靠性评定
	QJ 3250-2005	航天产品非工作状态可靠性设计与评价指南
方法标准	QJ 2398-1992	固体火箭发动机静止试验测试系统可靠性规范
	QJ 2631-1994	导弹系统级综合环境可靠性试验方法
	QJ 2653-1994	地-地战略导弹地面设备可靠性验证试验方法
管理标准	QJ 2345-1992	软件可靠性和可维护性管理

11.5.5 航空可靠性标准

航空标准是航空标准化机构根据航空产品的特殊要求按规定程序编制和审定的指令性（指导性）技术文件。航空标准涉及航空产品的设计、试制、试验、生产、使用和贸易活动，并有专业标识和编号。航空标准按照使用范围通常分为国际标准、区域标准、国家标准、国家军用标准、专业标准、企业标准等级别。中国的航空标准是航空方面的专业标准，标识为 HB。

航空可靠性标准的主要作用是：有利于保证和提高产品质量；缩短新产品的试制和生产准备周期；降低生产成本、合理利用资源、节约原材料；有利于开发新品

种、推广新技术；保证产品的互换性，便于维修和协作；有利于对外贸易和国际合作；有利于战时动员和装备部队。航空标准通常每隔 3~5 年复审一次，分别予以确认、修订或废止。

中国航空技术标准体系中有通用基础标准、零部件元器件标准、产品标准、质量管理与可靠性标准、工艺标准、材料标准、工艺装备标准、测试标准 8 大类。

国际航空航天标准的制定机构是国际标准化组织第 20 技术委员会。中国是这个技术委员会的成员国。中国航空工业的标准化工作始于 1957 年。中国航空标准化研究所是航空标准体系的制定和标准化的管理机构。

目前除了以上可靠性国际标准、国军标中给出的可靠性标准以外，现行航空领域主要的可靠性标准如表 11-17 所示。

表 11-17 航空领域主要的可靠性标准

标准类型	标准编号	标准名称
基础通用标准	HB/Z 123-1987	航空产品可靠性与质量信息表格
	HB 5830.1-1984	机载设备环境条件及试验方法总则
	HB 6167-1989	民用飞机机载设备环境条件和试验方法
产品标准	HB 7232-1995	军用飞机可靠性设计准则
	HB 7254-1995	直升机可靠性设计准则
	HB 7500-1997	空空导弹可靠性设计准则
	HB 7501-1997	机载导弹发射装置可靠性设计准则
	HB 5842-1990	航空产品特性、单元件分类及质量控制原则
质量管理标准	HB 6139-1987	航空机载设备可靠性试验（鉴定和验收）
	HB 7177-1995	军用飞机可靠性维修性外场验证
	HB 7592-1998	飞机非电子系统可靠性增长的试验方法
	HB 6158-1988	可靠性试验故障分类

参 考 文 献

[1] IEEE STD 982.1-1988. Dictionary of measures to produce reliable software. 1988.

[2] IEEE STD 982.2-1988. IEEE guide for the use of IEEE standard dictionary of measures to produce reliable software. 1988.

[3] IEEE STD 982.1-2005. Dictionary of measures of the software aspects of dependability. 2005.

[4] IEEE STD 1633-2008. IEEE recommended practice on software reliability. 2008.

[5] AIAA/ANSI R-013-1992. Recommended practice for software reliability. 1992.



- [6] ITAA STANDARD GEIA-STD-0009-2008, Reliability program standard for systems design, development and manufacturing, 2008.
- [7] 王光芦, 李维宝, 李大鹏. GEIA-STD-0009 系统设计、研制和制造可靠性大纲标准分析. 装备环境工程, 2011, 8 (6): 66~69.
- [8] 杜和青. 俄罗斯航天可靠性标准的分析和借鉴. 航天标准化, 1998, 1: 49~52.
- [9] 可靠性标准清单, <http://wenku.baidu.com/view/8ble05150b4e767f5acfce53.html>.
- [10] <http://www.kekaoxing.com>.
- [11] <http://www.docin.com/p-347797681.html>.
- [12] <http://www.doc88.com/p-0903761635538.html>.
- [13] <http://www.chinaer.org/info.aspx?n=20100611155627013527>.
- [14] <http://course.baidu.com/view/5d13660003d8ce2f00662399.html>.
- [15] <http://www.pv265.com/e/tags/?tagname=%BA%CB%B5E7%B3%A7>.
- [16] <http://www.nea.gov.cn/2011-10/31/c-131221292.html>.
- [17] <http://wenku.baidu.com/汽车电子环境可靠性相关标准介绍>.
- [18] <http://www.docin.com/p-255650708.html>.
- [19] 孙恒. 美国军用标准知识简介. 电子对抗技术, 1987, 6: 41~47.
- [20] 孙晓君. 军用可靠性保证标准综述. 电子产品可靠性与环境试验, 2012, 30 (1): 61~65.
- [21] 可靠性设计大全编撰委员会. 可靠性设计大全. 北京: 中国标准出版社, 2006.

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：(010) 88254396; (010) 88258888

传 真：(010) 88254397

E-mail: dbqq@phei.com.cn

通信地址：北京市海淀区万寿路 173 信箱

电子工业出版社总编办公室

邮 编：100036

